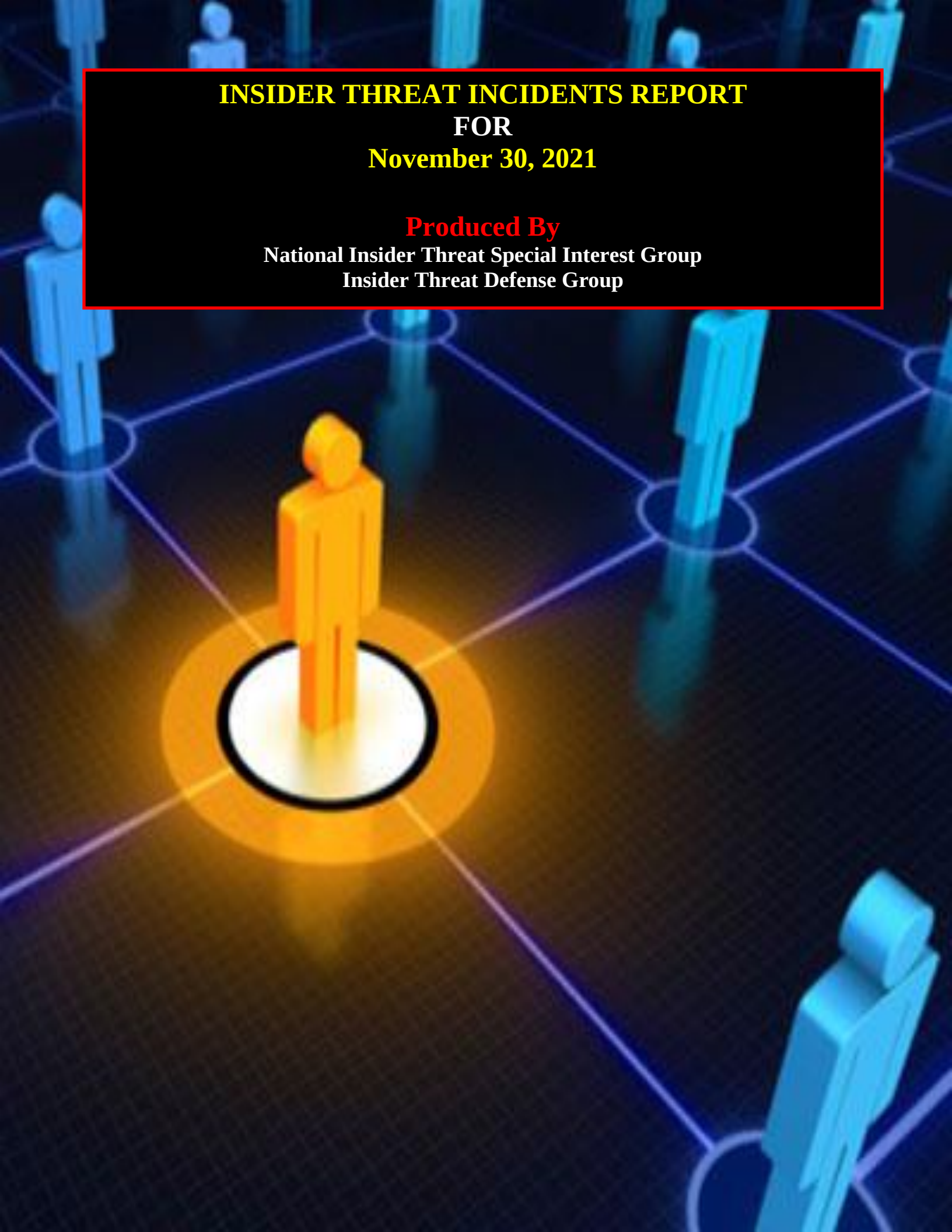

INSIDER THREAT INCIDENTS REPORT
FOR
November 30, 2021

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 **3,100** 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 24 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 NOVEMBER 2021

U.S. GOVERNMENT

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

Sean Okrzesik admitted that from February 2020 through February 2021, he opened bank accounts using the names and Social Security numbers of various Supplemental Security Income (SSI) beneficiaries or their representative payees. Okrzesik also admitted that once these accounts had been created, he would divert SSI benefit payments intended for these beneficiaries into the accounts, which he then used to pay personal expenses including the purchase of video gaming equipment, a custom suit, jewelry, airline tickets to the Caribbean, and online gambling. The total amount of SSI benefits stolen by Okrzesik was $103,798.77. (Source)

Former U.S. Postal Employee Pleads Guilty To Stealing Cash And 44 Gift Cards From Letters - November 1, 2021

Nathaniel Bonilla was a mail processing clerk at the U.S. Postal Service's Process and Distribution Center (PDC) in Hartford. Between April 2020 and October 2020, Bonilla opened mail envelopes with a razor blade and removed cash and dozens of gift cards or prepaid debit cards for his own personal use.

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

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

Former U.S. Postal Service Employee Pleads Guilty To Stealing $4,800+ From Mail - November 17, 2021

From August 2018 to October 2020, Colleen McAvoy was a part-time letter carrier for the USPS in Washington County, New York, based at the Cambridge Post Office. In pleading guilty, she admitted to opening mailed packages in order to steal U.S. currency, gift cards and lottery tickets contained inside of those packages. She admitted to stealing items worth a total of approximately $4,889.25. (Source)

U.S. Postal Contractor Employees Charged Following Seizure of 8,000+ Pieces of Stolen Mail Worth $4 Million+ - November 2, 2021

Two Lubbock postal contractors have been charged with possession of stolen mail. The investigation which culminated in the recovery of more than 8,000 pieces of mail worth more than $4 million, marks the largest ever seizure of stolen mail in Northern District of Texas history.

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

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

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Metallurgist Lab Director Pleads Guilty To Falsifying Test Results For Strength Of U.S. Navy Submarines Hulls - November 8, 2021

Bradken, Inc. is the U.S. Navy's leading supplier of cast high-yield steel for naval submarines. Bradken's Tacoma foundry produces castings that prime contractors use to fabricate submarine hulls. The Navy requires that the steel meets certain standards for strength and toughness to ensure that it does not fail under certain circumstances, such as a collision. For 30 years, the Tacoma foundry (which was acquired by Bradken in 2008), produced castings, many of which had failed lab tests and did not meet the Navy's standards.

Elaine Thomas, as Director of Metallurgy, falsified test results to hide the fact that the steel had failed the tests. Thomas falsified results for over 240 productions of steel, which represent a substantial percentage of the castings Bradken produced for the Navy.

Bradken's management was aware of the fraud until May 2017. At that time, a lab employee discovered that test cards had been altered and that other discrepancies existed in Bradken's records. (Source)

Former U.S. Army Employee Sentenced To Prison For Kickback Scheme To Steer $3 Million+ Of U.S. Government Contracts - November 10, 2021

A former civilian employee of the U.S. Army's Directorate of Public Works was sentenced to two years in prison for a kickback scheme to steer government contracts for work at Camp Arifjan, a U.S. Army base in Kuwait.

Ephraim Garcia admitted that he conspired with Gandhiraj Sankaralingam, the former general manager and co-owner of Kuwait-based contracting company Gulf Link Venture Co. W.L.L. (Gulf Link), to steer government contracts to Gulf Link.

In his position with the U.S. Army, Garcia was involved in the solicitation, award and management of certain government contracts related to facilities support at Camp Arifjan.

In 2015, at an Olive Garden restaurant located in Mahboula, Kuwait, Garcia and Sankaralingam approached an employee of the prime contractor responsible for base support services. During that meeting, they offered to pay the prime-contractor employee in exchange for his assistance in steering subcontracts worth over $3 million to Gulf Link. Rather than agree to the scheme, the prime-contractor employee reported the kickback offer to authorities. (Source)

Former Air Force Employee Sentenced To Prison For Stealing $1.1 Million+ Of Government Funds For Personal Use - November 29, 2021

From January 2003 to February 2018, Eddie Ray Johnson was a civilian Air Force employee, most recently as a travel coordinator in the Secretary of the Air Force, Office of Legislative Liaison, where he planned congressional travel and reviewed and approved accounting packages submitted by trip escorts, among other duties.

Johnson admitted that from March 2014 through September 2017, he used his government-issued travel credit card to obtain more than $1.1 million in cash advances, at least $774,000 of which he diverted to his own personal use. (Source)

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

From at least August 2016 through October 2019, Anthony Lesane, a police officer working for the Department of Defense at a facility in Prince George's County, Maryland, falsely recorded work hours in his department's time and attendance system that he had not worked. On most occasions, Lesane claimed to have worked overtime hours and on at least one occasion, Lesane claimed work hours while he was out of the country on vacation. Lesane stole at least $25,832.47 by over billing the DoD. (Source)

2 Department Of Veterans Affairs Employees Charged With Pocketing Over $250,000 In Cash From Vendors For Kickbacks - November 17, 2021

CHICAGO — Two employees of the U.S. Department of Veterans Affairs pocketed cash from vendors in exchange for steering them orders for medical equipment, according to indictments returned in federal court in Chicago.

Andrew Lee and Kimberky Dyson worked as Prosthetic Clerks in the Veterans Health Administration Prosthetics Service in Chicago. As part of their duties, Lee and Dyson selected vendors from which to order medical equipment for VA patients, and then paid the vendors using government purchase cards. In exchange for their efforts with certain vendors, Lee and Dyson allegedly received cash payments from individuals at the vendor companies, in exchange for steering them orders for medical equipment. Lee pocketed kickbacks of at least $220,000. Dyson accepted at least $39,850. (Source)

Former Defense Logistics Agency Supervisor Pleads Guilty To Sexual Assaulting Subordinate Employee - November 2, 2021

Jared Heisey is a former Defense Logistics Agency (DLA) supervisor. He admitted to assaulting a subordinate employee during work hours on August 9, 2019, at the NSA. Heisey admitted he directed the victim to accompany him to conduct an inventory count in a remote building at the Naval Support Activity and when they entered the building, Heisey pinned the victim up against the wall by grabbing her neck with his hand while making sexual comments about what he would like to do to her. Heisey was subsequently terminated and is no longer employed by DLA. (Source)

Former Pharmacy Chief Of Veterans Affairs Medical Center Pleads Guilty To Diverting Painkillers - November 12, 2021

Matthew Camera, 50, pleaded guilty to one count before United States District Judge Susan Paradise Baxter.

In connection with the guilty plea, the court was advised that from January 2017 to June 2020, while Matthew Camera was employed as the Pharmacy Chief at the Veterans Affairs Medical Center in Erie, PA, he unlawfully obtained multiple dosage units of Hydrocodone and Oxycodone from pill bottles awaiting delivery to Veterans Affairs patients. (Source)

Former Freight Company Executive Admits Role In $550,000+ Embezzlement Scheme Involving DoD & Egypt - November 16, 2021

Morten Nielsen was a program manager for a freight forwarding company, Nielsen was responsible for the company's contract relating to the Egyptian Foreign Military Sales program (EFMP), a program between the government of Egypt and the U.S. Department of Defense (DoD) that facilitated the sale and repair of military equipment from the DoD to Egypt.

From July 2017 through July 2019, Nielsen submitted fraudulent invoices from a sham company that he controlled to the freight forwarding company for work that the sham company never performed. Nielsen then sent the fraudulent invoices on behalf of his employer to the Egyptian government. The fraudulent invoices were approved by Egypt and, in turn, the DoD reimbursed the freight forwarding company. Nielsen caused his employer to pay the sham company he created approximately $559,000 over the course of two years, and then transferred those funds into his personal account. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former Mayor Sentenced To Prison For Corruption / Accepting $5,000 Bribe - November 10, 2021

Dennis Tyler served as the Mayor of Muncie, Indiana from 2011 to 2019, during which he oversaw various public works projects. In December of 2015, Tyler took $5,000 in cash from a local excavation contractor in exchange for awarding public works projects to that contractor, passing up lower bids or more qualified contractors. Tyler received the money in a parking lot from former Muncie Superintendent of Sewer Maintenance and Engineering, Tracy Barton, who delivered the cash on behalf of the contractor. Barton has also been charged in this investigation.

In total, the City of Muncie and the Muncie Sanitary District awarded the excavation contractor hundreds of thousands of dollars in contracts for city work in connection with kickbacks paid to Tyler and Barton, including work associated with the Nebo Commons commercial development and the construction of a large sporting goods store.

Also, according to court documents, Tyler received a personal benefit from a different city contractor in early 2015. The contractor performed tree removal work at Tyler's personal property worth approximately $1,800, with the expectation that doing so would keep the contractor on a list of eligible bidders for city work. (Source)

Former City Employee Charged In $636,000+ COVID Relief Funds Fraud Scheme - November 4, 2021

John Bernardo had been employed by the City of West Haven as a Housing Specialist in the office of Community Development Administration. Michael DiMassa was employed as an Administrative Assistant to the City Council and was a Connecticut State Representative elected to represent West Haven and New Haven.

In January 2021, DiMassa and Bernardo formed Compass Investment Group, LLC. Beginning in February 2021, Compass Investment Group LLC fraudulently billed the City of West Haven and its "COVID-19 Grant Department" for consulting services purportedly provided to the West Haven Health Department that were not performed. From February 2021 through September 2021, the City of West Haven paid Compass Investment Group a total of $636,783.70. It is alleged that Bernardo received at least $45,000 of these funds. (Source)

Former State Employee Sentenced To Prison For Conspiracy To Illegally Import Prescription Drugs - November 2, 2021

Howard Head is a former Kentucky state employee. From July 2015 to October 2019, Head regularly made online purchases of thousands of tablets of erectile dysfunction drugs, from overseas suppliers. These drugs were not authorized for entry into the United States and did not satisfy Food and Drug Administration regulations for proper labeling. Additionally, Head is not a doctor or pharmacist, and had no legal authority to prescribe, dispense, transport or otherwise handle prescription medications.

After obtaining the shipments of generic erectile dysfunction drugs, Head resold them at a profit, to customers in various parts of Kentucky. While operating this illegal business, in some instances,

Head used his state email account to order shipments and contact customers. He was also fined $1,000 and ordered to forfeit $30,275 in unlawful gains. (Source)

Former School Principal Pleads Guilty To $250,00 Of Wire Fraud Over 9 Years - November 1, 2021

Todd Wessels was a former curriculum and technology director and principal who stole at least $250,000 from a private, religious, not-for-profit school.

Wessels was responsible for ensuring that the school district met the technology needs of approximately 1,800 students at its high school, middle school, and elementary schools. Before 2016, Wessels also served in a dual role as the principal of one of the elementary schools.

Beginning on an unknown date but no later than June 2011, Wessels devised and executed a scheme to make purchases for his own benefit with the school district's funds. Wessels made purchases of pre-paid debit cards using the school district's store credit cards at area businesses upon the false and fraudulent pretense that he needed funds for "apps" for students' computers.

Wessels then electronically transferred the balances of the pre-paid debit cards to another account that he controlled at PayPal. Wessels had, without the school district's knowledge, falsely and fraudulent opened the PayPal account in the school district's name but under the handle "WENWESS". Wessels provided the school district receipts for the purchases of the pre-paid debit cards on the false and fraudulent pretense that the use of the store credit cards was for legitimate purchases. Wessels also sold the school district's computer equipment on third-party Internet websites without its knowledge or permission.

In July 2019, a new chief administrator at the school district began looking into Wessels's spending practices. Wessels repeatedly lied to administrators and submitted fraudulent invoices and receipts to them in order to conceal his scheme to defraud. At meetings in January and February 2020, Wessels provided hardcopy versions of false, fraudulent, and fictitious spreadsheets purporting to show the apps he had purchased. (Source)

Former School Bookkeeper Sentenced To Prison For Embezzling $121,000+ - November 2, 2021

Carlina Moore was employed by the Montessori Educational Center, Inc. (MEC) as a bookkeeper from May 2018 to August 2020 and she handled all in-house bookkeeping for them.

On or about August 25, 2020, the MEC's administrator reviewed their bank account and discovered a questionable transaction. This prompted the administrator to conduct a further review of the bank and credit card accounts. Their investigation into the questionable transaction revealed that Moore was embezzling funds from the MEC's accounts without their knowledge or authorization.

Law enforcement agents further investigated the fraudulent activity and confirmed that Moore had in fact defrauded the MEC by transmitting funds by way of wire communications in interstate commerce. Moore admitted that she devised a scheme to defraud the MEC and that she did so in order to obtain money and property from the MEC fraudulently and for her own personal gain. She admitted that she embezzled $121,600.50 from the MEC. (Source)

Former Supervisor County Tax Commissioner's Office Was Paid $20,000 In Bribes To Illegally Register Vehicles - November 1, 2021

From July 2017 to November 2019, Gerald Harris served as the Supervisor of Tax Tag Clerks for the DeKalb County Tax Commissioner's Office. In that position, Harris oversaw the Tax Commissioner North Office's clerks who processed motor vehicle registrations and renewals for customers.

From at least May 2019 to November 12, 2019, Lesbia Lily Gonzalez Moreno repeatedly paid Harris bribe payments to register unlawfully vehicles for owners who did not present a valid Georgia driver's license or identification card. In exchange for bribe payments, typically $200 per vehicle, Harris unlawfully registered and obtained license plates for owners identified by Moreno. In many cases, Moreno paid bribes to register vehicles for people who presented only foreign identification documents. During this period, Moreno paid Harris more than $20,000 in bribe payments. (Source)

Former Director Of Finance For School District Charged With Embezzling $90K+ In District Funds - November 30, 2021

From November 2013 until July 2019, the Christopher Gehris was the Director of Finance / Business Manager of the Phoenixville Area School District (PASD). Gehris misappropriated funds from PASD bank accounts, directed unauthorized payments to himself, made false entries, and fabricated receipts, all in order to embezzle more than $90,000 in school funds earmarked for student sporting events, field trips, summer programs and other school events. (Source)

FOREIGN GOVERNMENT ESPIONAGE

Cleaning Person For Israeli Defense Minister Charged With Espionage - November 18, 2021

Israel has charged the housekeeper for the country's defense minister with espionage for offering to spy for hackers reportedly linked to Iran, Israeli officials said.

The man, identified as Omri Goren, reportedly has a criminal record but worked at Defense Minister Benny Gantz's home as a cleaner and caretaker.

How he got close, personal access to an Israeli leader with security clearance remains something of a mystery, even to experts. The incident raised questions about how thoroughly such workers are vetted. The Shin Bet Security Service, which announced the arrest, said it was reviewing its vetting procedures.

Goren saw reports in the Israeli media about a hacker group called "Black Shadow." He looked up the group and used the Telegram app to contact one of its agents, presenting himself as someone who worked for Gantz. Goren demonstrated his access to the defense minister by sending photographs of various items in Gantz's home, including his computer.

Goren discussed infecting Gantz's computer with malware but was arrested before any plans were carried out.

Goren's public defender was quoted in news reports as saying the suspect was desperate for money and had no intention of damaging national security.

Israeli media reported that Goren has been sentenced to prison on four occasions, including for armed robbery and breaking into homes. According to the reports, he did not undergo a security review before working for Gantz. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

Former Police Officer Sentenced To Prison For Conspiracy To Commit $1 Million+ Wire Fraud / Bank Fraud Scheme With 10+ Co-Conspirators - November 2, 2021

From approximately January 2015 through January 2017, while he was employed as a Clayton County, Georgia police officer, Andre Jackson conspired with others to commit wire fraud and bank fraud.

Jackson and his coconspirators recruited more than 10 individuals with good credit, ncluding some of Jackson's fellow police department employees to apply for loans to purchase luxury vehicles from automobile dealers in the Northern District of Georgia and the Southern District of Texas.

Jackson and his coconspirators told the straw purchasers that they planned to sublease the vehicles to individuals who had significant incomes but poor credit. Jackson and his coconspirators also told the straw purchasers that one of Jackson's coconspirators owned a car-leasing business, which would be responsible for servicing the vehicles, obtaining and paying for insurance on the vehicles, and paying the monthly loan payments. Jackson and his coconspirators promised to pay each straw purchaser as much as $5,000 for every loan they obtained.

Jackson and his coconspirators caused the straw purchasers to submit loan applications that contained false and fraudulent information concerning their income and employment.

Jackson was ordered to pay $1,011,989.87 in restitution. (Source)

8 Civilian Employees Of Philadelphia Police Department Charged With Theft And Fraud Charges For Collecting Pandemic Unemployment Assistance - November 23, 2021

7 of the 8 defendants are employed as radio dispatchers for the Philadelphia Police Department (PPD).

Each of the defendants is alleged to have submitted weekly certifications stating that they were not employed and were ready, willing, and able to work each day. The Indictments charge that these statements were false because each defendant was employed at the time by PPD. As part of the weekly certifications, each defendant also certified that he or she was not earning any wages or grossly unreported true wages to secure eligibility. However, these statements are also allegedly false according to PPD payroll records. As a result of these false statements, each defendant received Pandemic Unemployment Assistance funds for multiple weeks in which he or she also collected his or her PPD salary. (Source)

Former Detroit Police Department Officer Pleads Guilty To Taking $3,200 In Bribes - November 16, 2021

From in or about July 2019, and continuing through in or about May 2021, Alonzo Jones corruptly accepted approximately $3,200 in bribes with the intent to be influenced and rewarded in connection with his duties overseeing and running the Detroit Police Vehicle Auction. (Source)

Former Sheriff's Office Captain Sentenced To Prison for Defrauding Sheriff's Office And Other Businesses Of $241,000 - November 12, 2021

A former A New Orleans Tangipahoa Parish Sheriff's Office (TPSO) Captain Kevon Stimage wa sentenced to 12 months of imprisonment, 1 year of supervised release. Stimage pled guilty to theft from programs receiving federal funds.

In 2017, 2018, 2019, and 2020, Stimage reported having worked, on average, 40 hours per week at the TPSO, approximately 40 hours per week at an off-duty work detail at a motor vehicle dealership, and, beginning in 2018, approximately 30 hours per week at an off-duty work detail at an apartment complex, for a total of approximately 110 hours per week. However, Stimage only worked a portion of the claimed hours, thereby defrauding the TPSO, the vehicle dealership, and the apartment complex out of a total of $241,086. (Source)

Former Police Officer Sentenced To Prison For $95,000 Bribery Scheme To Protect Brothels - November 3, 2021

From September 2014 to August 2015, Julio Rivera solicited and accepted cash payments from a Newark brothel owner who ran brothels. In exchange for these cash bribes, Rivera violated his lawful duties for the benefit of the brothel owner, including declining to arrest individuals who were committing and promoting prostitution, agreeing to protect these individuals from arrest by other police officers, and agreeing to take adverse action against a competing brothel. Rivera collected between $40,000 and $95,000 in bribes in exchange for protecting those and other brothels. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Employee Sentenced To Prison For Embezzling $450,000 Over 8 Years For Personal / Family Use – November 18, 2021

Lisa Stabeno admitted that she began embezzling from the church in November 2013, just four months after assuming accounting responsibilities.

Stabeno began by using two credit cards, one assigned to a church employee and one assigned to a pastor to pay personal expenses, including a car loan she co-financed with her daughter, medical and dental expenses, clothing, salon services, and restaurant meals. She also used the credit cards to purchase supplies for a bakery she co-owned with her daughters.

Beginning in 2014, Ms. Stabeno began making payments to herself with church credit cards using Square, a digital point-of-sale payment system which processes payments from credit cards run through a port connected to a cell phone.

In 2015, Ms. Stabeno opened two credit cards, one in her own name and one in her daughter's name, which she used for personal expenses. She then paid off hundreds of thousands of dollars in credit card debt on the cards using money from church bank accounts.

She also used the personal credit cards to make purchases and payroll at her bakery, then paid off the cards with money from the church accounts, thus boosting the bakery's sales and profits and raising her daughters' salaries. (Source)

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

Former Pfizer Employee Stole Covid Vaccine Trade Secrets / Had Received Employee Offer From Xencor - November 24, 2021

Chun Xiao (Sherry) Li allegedly uploaded more than 12,000 files including scores of documents with confidential information to a Google Drive account, Pfizer alleged. The documents are said to pertain to a broad range of topics, including analysis of vaccine studies, operational goals, and development plans for new drugs.

Pfizer said in the complaint it believed Li was going to Xencor Inc. and that she provided a decoy laptop when confronted about subsequent downloads of the information.

Pfizer already had disabled USB access in 2019 to prevent unauthorized file transfers. In October 2021 it also implemented a technology that monitors when employees upload files to cloud-based platforms like Google Drive, according to the complaint. It said it detected Li transferring 12,000 files from her Pfizer laptop to an online Google Drive account in a three-day window in October.

A digital review of Li's Pfizer email revealed she had been interviewed and received an employment offer from Xencor, Pfizer said. When confronted Li admitted transferring the files and claimed she did so to organize her files offline for her personal use but hadn't copied them or sent them elsewhere.

Pfizer alleged that between conversations with Pfizer forensics personnel held hours apart, Li deleted all of the files saved on her Google Drive account. She allegedly disclosed the deletions in the second meeting, at which point Pfizer asked for her to hand over her external hard drive and personal laptop.

The forensic investigation revealed the laptop she turned in wasn't the one that downloaded the 12,000 files, largely because it was lightly used during the week of the downloads, Pfizer said. The examination showed a significant number of documents were deleted from her hard drive before she turned it in, according to the complaint. (Source)

Former Hospital Nurse Sentenced To Prison For Obtaining And Tampering With Opioid Pain Killer For Personal Use - November 1, 2021

Nathan Pehrson was a nurse on a surgical and trauma ward at a hospital. Pehrson diverted the pain killing narcotic hydromorphone from pre-loaded syringes for his personal use, and then replaced the pain medication with saline solution before they were placed back into circulation for medical use by other hospital staff on other patients. (Source)

Former Medical Center Nurse Charged With Removing Controlled Substances In Hospital Storage - November 1, 2021

Alec Ramirez who was a registered nurse, is accused of removing vials of fentanyl and hydromorphone from an automated dispensing cabinet at Menorah Medical Center in Overland Park and replacing the substances with an alternate liquid then returning the vials to the cabinet. (Source)

TRADE SECRET THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former General Electric Company (GE) Engineer Sentenced To Prison For Conspiring To Steal Trade Secrets Over 11 Years - November 10, 2021

As part of his guilty plea entered on December 10, 2019, Jean Delia admitted that he conspired with his business partner and co-defendant, Miguel Sernas, to compete against GE using trade secrets Delia stole from GE while employed by GE in Schenectady, New York. Delia admitted that he and Sernas, operating as ThermoGen Power Services, used the stolen trade secrets, as well as stolen marketing data, pricing information, and other confidential GE documents, to compete against GE around the world.

Delia, who was employed by GE as an engineer from 2001 through 2012, admitted to conspiring with Sernas from 2008 through 2019. (Source)

Jury Convicts Chinese Official Of Espionage For Attempting To Steal Trade Secrets From GE Aviation With Help Of GE Employee - November 9, 2021

Yanjun Xu is a deputy division director at the Chinese Ministry of State Security (MSS), which is the intelligence and security agency for China.

Beginning in at least December 2013, Xu targeted specific companies in the United States and abroad that are recognized as leaders in the field of aviation.

He identified individuals who worked for the companies and recruited them to travel to China, often initially under the guise that they were traveling to give a presentation at a university. Xu and others paid the individuals stipends on top of covering travel costs.

Xu attempted to steal technology related to GE Aviation's exclusive composite aircraft engine fan, which no other company in the world has been able to duplicate, to benefit the Chinese state.

In March 2017, a GE Aviation employee in Cincinnati was solicited to give a report at a university in China. The employee traveled to China two months later to present at the university and was introduced to Xu. Xu and others paid the employee's travel expenses and a stipend.

In January 2018, Xu requested "system specification, design process" information from the employee and – with the cooperation of the company, who was working with the FBI – the employee emailed a two-page document from the company that included a label that warned about the disclosure of proprietary information.

In February 2018, Xu began discussing with the employee the possibility of meeting in Europe during one of the employee's business trips and asked the employee to send a copy of the file directory for his company-issued computer. (Source)

Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company - November 9, 2021

Peter Kim worked as a principal design engineer at Broadcom forr over twenty years. Broadcom is headquarted in San Jose and its products include networking chips used in equipment sold worldwide, including for enterprise and data center networking.

In the days before his July 17, 2020, departure from Broadcom, Kim stole Broadcom trade secrets from the company that were associated with a Broadcom family of chips often used in high-volume data centers.

About 10 days after his departure from Broadcom, Kim began working at the new company at the director level. His new employer was a China-based startup company focused on chip design and the market for networking chips. Kim received a laptop for his work at the new company, and, during the 9 months following his departure from Broadcom and the start of his work at the new company, Kim repeatedly used Broadcom trade secrets on the newly-issued laptop and on other electronic devices. These trade secrets were associated with test plans, design verification environment files, and design specifications for the Broadcom family of chips. (Source)

Former Employees Of Taiwan Company Caught Selling Trade Secrets To China For Millions - November 14, 2021

Taiwan Police have opened a probe into two ex-employees of a optoelectronic device maker for allegedly stealing trade secrets and selling them to China.

The police received tip-offs about the theft back in March from the company's Chief Executive who discovered that confidential material was being stolen. As they started investigating, they found that two former employees at the had made millions from selling confidential information.

Analyses of the firm's computer systems revealed that both the ex-employees had downloaded sensitive material for years unitil one quit his job, and the co-founder of the company resigned. earlier.

Among the stolen material was product designs, system analyses, testing procedures, parts purchasing databases and other confidential files. (Source)

BANKING / FINANCIAL INSTITUTIONS

3 Bank Employees / 8 Others Charged In Counterfeit Checks And Bank Fraud Schemes - November 22, 2021

11 individuals, including 3 bank employees have been charged with participating in schemes to defraud local banks by creating and depositing checks, then withdrawing bank funds prior to financial institutions discovering the fraudulent activity. The counterfeit checks contained personal account information belonging to, among others, individuals, small businesses, an insurance company, and an attorney's office. (Source)

Former Bank Manager Sentenced To Prison For $450,000+ Of Bank Fraud - November 16, 2021

Kazi Pervez was a branch manager for a bank in Salem, New Hampshire. From at least April of 2016 until September of 2017, Pervez used his position as branch manager to steal or attempt to steal more than $560,000 from the bank. Pervez opened or instructed bank employees to open accounts in the name of deceased bank customers. Pervez then withdrew funds from the accounts that exceeded the balance of the accounts and used his authority as branch manager to authorize the overdrafts from the account. Pervez also identified inactive bank accounts of deceased bank customers and transferred money out of those accounts to other accounts that he controlled.

Pervez transferred the funds he stole or overdrew between several accounts in the bank that he controlled before transferring the money to accounts at other banks or to pay his bills. In total, Pervez stole or fraudulently overdrew about $564,590.02 from other peoples' bank accounts. Of that amount, Pervez successfully transferred more than $450,000 to other accounts outside the bank for his personal use. (Source)

3 Bank Employees Arrested For Committing $850,000+ Of Financial Crimes - November 4, 2021

Brady Torgerson, while employed at two separate North Dakota financial institutions, engaged in a scheme to defraud both financial intuitions by issuing bank funds to individuals not entitled to these funds, failing to register banking transactions, creating fraudulent loan obligations, and taking actions to conceal his activities. Brent Torgerson, the father of Brady Torgerson, while employed at a North Dakota financial institution, misapplied bank funds by issuing a $724,558.48 cashier's check to his son, Brady Torgerson, without obtaining promissory notes and other necessary financial paperwork.

Kelly Huffman, while employed at a North Dakota financial institution, misapplied bank funds by unlawfully issuing a $125,648.64 check advance to a separate North Dakota financial institution at Brady Torgerson's request. (Source)

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

Former Employee (Wife) Sentenced To Prison For $145,000 Payroll Fraud Scheme Involving Husband Who Also Worked For Same Company - November 1, 2021

Melissa Sepulvado and her husband were employed by Weyerhaeuser Company. Melissa Sepulvado was a Senior Support Specialist and had been with the company for 17 years, and her husband was employed as an hourly worker.

Melissa Sepulvado's primary duties were to review and approve payroll entries for the hourly workers at Weyerhaeuser through its internet based, electronic payroll system. In addition, she reviewed vacation payout requests by hourly workers.

From November 2014 to April 2017, Melissa Sepulvado defrauded Weyerhaeuser of $145,000 by exploiting her position and access to the payroll system. She regularly entered vacation payout requests for her husband for hours he did not earn, and although she was not supposed to review or approve her husband's pay requests, she did approve them. Weyerhaeuser then deposited money into her husband's bank account based on the fraudulent pay requests.

Melissa Sepulvado took steps to conceal the fraud by backdating numerous vacation payout requests, entering the requests for completed pay periods from months or years earlier. These actions concealed the requests from regular audits of the system. (Source)

Former Office Manager Admits To Embezzling $350,000+ From Home Healthcare Agency / Elderly Clients - November 24, 2021

Ana Phimmasone admitted that from April 2016 until April 2018, she stole $352,594.47 from a local company that provides in-home care services for mostly elderly individuals, as well as from several of its clients.

Between April 2016 and August 2016, Phimmasone embezzled $25,958.60 by stealing checks that were issued by, or belonged to, her employer, and deposited them into her own bank account. Then, between December 2016 and April 2018, Phimmasone exploited her access to clients' credit card information by billing them using PayPal, Venmo, Square and Apple Pay and diverting the money to her own accounts instead of using the funds to pay her employer for the in-home care services.

To make the fraudulent charges appear legitimate, Phimmasone falsely told the victims that the healthcare provider changed its existing payment processing company to PayPal. After receiving the funds, Phimmasone spent the money or diverted the payments into her personal bank accounts.

To disguise the illegal transfers and avoid detection, Phimmasone created a fraudulent PayPal account using the name and personal information of C.P., an 87-year-old individual. Phimmasone then used the fraudulent PayPal account to bill the other victims' credit cards, causing victims to believe they were being charged for legitimate medical care. (Source)

Former Property Manager For Ranch Charged With $421,000+ Of Wire Fraud - November 23, 2021

Maria Southall-Shaw was the former manager of Shadow Creek Ranch in texas. First Service Residential (FSR) is Shadow Creek's property management company and employed Southall-Shaw.

She allegedly engaged in a scheme to defraud FSR. Between December 2013 and November 2017, she approved invoices from a ranch vendor for goods and services she knew the vendor had not provided.

Southall-Shaw allegedly caused this vendor to kickback to her 50% of the payment the vendor received, which totaled $421,519. (Source)

Former President Of Produce Market Sentenced To Prison For Stealing $8 Million+ From Company To Pay Beach House Rent, Friends, Etc. - November 22, 2021

Caesar DiCrecchio is the former President and CEO of the Produce Market.

He defrauded the Market by using company funds to pay $1.9 million in rent on his Stone Harbor, New Jersey shore house; converting into cash $1.1 million in checks drawn on the Market's bank account and using the cash for his own benefit; causing $1.7 million in checks to be issued from the Market operating account payable to his friends or relatives; causing the Market to pay for the defendant's personal credit card expenditures; converting $320,000 in checks that were payable to the Market and cashing them for his own benefit; skimming $2.6 million in cash from the pay gate at the Market's parking lot, which he used to pay Market employees 'under the table' while keeping a substantial portion for his own use; and using Market funds to provide a $180,000 loan to a Market vendor, which the vendor repaid directly to DiCrecchio.

DiCrecchio concealed these expenditures in the Market's books and records by directing that these payments be reflected as legitimate business expenditures. (Source)

Former Contract Bookkeeper Sentenced To Prison For Embezzling $150,000+ From High-End Mountain Bike Company For Gambling - November 22, 2021

Joan Trower worked as a contract bookkeeper and accountant for the mountain bike company from July 2015 to May 2018. Her contract was terminated when the embezzlement was discovered.

Trower used a variety of schemes to steal over $150,000 from company accounts: creating checks using the company software system, forging signatures, claiming expenses and compensation she did not earn, and making transfers from company accounts to accounts she controlled in the names of phony tax accounting businesses.

While most employees received at most 3 checks per month (2 For Salary, 1 For Expenses), Trower wrote as many as 13 checks to herself in one month. Trower put false descriptions in the memo line, sometimes falsely claiming the funds were to reimburse her for an outside tax accounting firm she claimed to have hired. Trower also transferred money from company accounts to accounts she controlled, transferring more than $26,000 to her account in the span of just a few months in 2018. Trower and her boyfriend used the money to, among other things, gamble at area casinos.

Trower committed aggravated identity theft when she forged the signature of company executives on fraudulent checks and when she submitted false invoices in the name of a third-party tax accountant to justify reimbursements to Trower. (Source)

Former Bookkeeper Charged For Embezzling $200,000+ From Business For Personal Use - November 19, 2021

Kimberly Hodge was the bookkeeper for Integrity Architectural Millwork (Integrity) and was responsible for, among other duties, making Quickbooks entries and recording payments to vendors. Between February 2019 and April 2020, Hodge fraudulently made deposits into her personal bank account from the operating account of Integrity and caused fraudulent payments to be made to her account from Integrity's credit card.

In February 2020, Hodge forged the name and signature of the owner of Integrity to apply for a loan from a financial institution in the amount of $150,000 to replenish the funds in the Integrity operating account to conceal the fraud. In the loan application, Hodge provided the owner's personal information, including a photo of the owner's driver's license.

In April 2020, Integrity applied for and received a loan in the amount of $127,447 from the Payroll Protection Program (PPP) of the Small Business Administration, under the Coronavirus Aid, Relief, and Economic Security Act. These funds were intended to be used for employee salaries and business expenses of Integrity during the COVID-19 pandemic. The indictment alleges that Hodge also transferred funds from the PPP account to the Integrity operating account to conceal her fraud. In May 2020, Integrity discovered the fraud and terminated Hodge's employment, after which she continued to attempt to make fraudulent purchases using Integrity's credit card.

The indictment also contains a forfeiture allegation in which the government seeks a money judgment of at least $209,443.63, which represents the proceeds of the crimes committed. (Source)

Former Administrative Assistant / Bookkeeper Sentenced To Prison For $335,000+ Of Wire Fraud From Employer For Personal Expenses - November 18, 2021

The charges against Tracice Sonnier stemmed from an investigation that began when her employer discovered money missing from their business account.

Sonnier was employed by Aries Marine Corporation (Aries) from 1996 until her termination in May 2020. She worked as an administrative assistant and had bookkeeping duties at Aries.

Sonnier created a scheme to defraud Aries using Aries' bank accounts, without authorization, to pay for personal expenses. The investigation revealed that her scheme resulted in a loss to the company of $335,015.67. (Source)

Former Office Manager Charged With Wire Fraud For Stealing $1 Million+ From Employer Over 8 Years For Personal Use & Husbands Business - November 18, 2021

Tammy Moore was an Office Manager for a company that made custom components for a variety of industries.

Between 2012 and 2020, Moore 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. (Source)

Former Financial Controller Charged With Embezzling $3 Million+ For Personal Use, Family, Friends - November 18, 2021

From May 2017 through the end of 2019, Rosalba Meza allegedly made unauthorized transfers estimated to total $3,071,880 from bank accounts belonging to Trilogy Plumbing, Inc. and a related company called Matrix Management, LLC.

In February 2019, Meza told executives their companies did not have funds to meet payroll obligations and failed to inform the executives that she had been embezzling from the companies.

Several months later, while the companies were the subject of an IRS enforcement action because of unpaid payroll taxes, Meza falsely told the executives that she did not pay the quarterly payroll taxes because she instead had used those funds to pay employees.

Once the funds were transferred to her accounts, Meza used the stolen money to make approximately $292,137 in cash withdrawals at bank branches and more than $1 million in withdrawals at ATMs in the United States and Mexico. Meza also allegedly wired approximately $870,209 to bank accounts in Mexico owned by a family member and another $250,000 in transfers to other family members and friends. (Source)

Former Company Accountant Charged For Embezzling $362,000+ From Employer - November 18, 2021

Carrie Long was employed by Executive Coach Builders, Inc. to provide in-house accounting services to the company and to Executive Bus Builders, Inc. The companies are headquartered in Springfield but do business worldwide with factories and sales offices in Missouri and California. The companies build luxury buses, coaches, and limousines. Long was hired in April 2014.

Long stole at least $362,175 from the companies from February 2016 to September 2020.

Long allegedly used her position as an in-house accountant for the companies, and her access to the companies' check stock, to regularly write checks against the companies' bank accounts for unauthorized payments to herself. Long stole money from the companies by filling in unauthorized amounts on some pre-signed checks and making such checks payable to herself. Long also allegedly stole money from the companies by forging signatures on the companies' checks, filling in unauthorized amounts on the checks, and making such checks payable to herself. (Source)

Former General Manager Of Food Services Company Charged Accepting $400,000 In Bribers And Tax Fraud - November 18, 2021

From 2014 through 2017, Mark Holmes, was the General Manager of a Pennsylvania food services company, He accepted approximately $400,000 in bribes and kickbacks from two temporary staffing companies, in exchange for their hiring employees. The two temporary staffing companies, in turn, received approximately $7,800,000 from Holmes's employer.

Holmes also was charged with failing to remit employment taxes to the IRS for a separate temporary staffing company, Encore Staffing Solutions LLC that he owned and operated with other coconspirators.

From March 2018 through December 2020, Holmes and his co-conspirators allegedly failed to pay approximately $135,000 in employment taxes owed by Encore Staffing Solutions LLC to the IRS. (Source)

Former Employee Charged With Stealing $1.8 Million+ In Bank, Wire Fraud, Identity Theft Scheme Over 7 Years - November 10, 2021

Between December 2013 and April 2020, Joanne Dinoto stole more than $1.8 million from her employer, a flooring company based in Boston.

Dinoto inflated her compensation by increasing her hourly rate, falsifying the number of hours she worked and adding phony "reimbursements" to her paycheck, all without authorization. Dinoto used her employer's corporate credit card for personal expenses, even after her employer directed her to cancel the card, and forged at least two checks to herself from her employer's checking account. To conceal the scheme, Dinoto allegedly modified her employer's accounting records. (Source)

Financial Secretary - Treasurer For United Auto Workers Union Charged With Embezzling $2 Million+ For Gambling, Automobiles, Firearms, Vehicles - November 10, 2021

Between 2011 and 2021, Timothy Edmunds has served as the Financial Secretary-Treasurer of Union Local 412 of the International Union, United Automobile, Aerospace, and Agricultural Workers of America (UAW).

Edmunds systematically drained the Local 412 accounts of about $2 million by (1) using Local 412 debit cards for over $142,000 in personal purchases, (2) cashing Local 412 checks worth $170,000 into accounts he personally controlled, and (3) transferring $1.5 million from bone fide Local 412 accounts into accounts that he personally controlled.

Edmunds has used portions of the proceeds of his embezzlement to gamble extensively, to purchase firearms, and to purchase various high-end vehicles. For example, between 2018 and 2020, Edmunds used the UAW Local 412 debit card to make over $30,000 in unauthorized withdrawals at the Greektown Casino. While gambling at the Greektown Casino, records indicate that Edmunds had cash buy-ins of over $1 million, and he put over $16 million in play while betting while being rated at the casino. Between 2020 and the present, Edmunds registered at least 10 firearms, which ranged in price between $500 and $2,000 per firearm. In February 2016, Edmunds purchased a 2016 Jeep Grand Cherokee SRT for $74,365. In July 2020, Edmunds purchased a 2020 Jeep Grand Cherokee Trackhawk, for $96,419. Subsequently, in July 2021, Edmunds purchased a 2021 Dodge Durango for $76,491. Edmunds also leased two 2021 Jeep Grand Cherokee Limited in December 2020. (Source)

Former Office Manager For Dermatology Practice Sentenced To Prison For Embezzling $350,000 Over 8 Years For Travel / Personal Use - June 4, 2021

From July 2012 to February 2020, Patricia Doucet defrauded her former employer, the Dermatology & Laser Center of San Antonio. The medical practice's owner and operator organized and conducted a non-profit educational symposium on regenerative medicine in San Antonio in 2012. A bank account was established to collect contributions for the symposium event. That account was to be closed at the conclusion of the symposium. But Doucet, in her capacity as office manager, kept the account open without permission.

In July 2012 to February 2020, Doucet began to embezzle checks and cash paid to the dermatology practice by depositing them into the symposium account. She altered a signature stamp utilized by the practice for its business account or fraudulently endorsed checks by forging the owner's signature.

Doucet also stole money from the practice's profit-sharing account that was designed to automatically issue checks to cover taxes for the employee's profit share. Rather than directing those checks to the IRS, Doucet instead deposited those checks into the symposium account.

Doucet then used the symposium account as her slush fund for international and domestic travel, property payments, meal purchases and other personal expenses on credit cards she fraudulently opened in the owner's name. (Source)

Former Office Administrator Admits To Embezzling $650,000 From Employer - November 5, 2021

Tina Wood was hired in 2013 by a supply company as an office administrator and secretary. Wood eventually was placed in charge of depositing payments from customers and given access to the company's accounting system. Wood used the accounting software to embezzle checks from one of the company's biggest customers and deposited most of the embezzled money into a personal bank account she opened in a bank. In February 2019, when the company's owner realized something was amiss, he contacted Wood. Wood refused to talk to the owner and cleaned out her desk the next weekend. An investigation found 109 customer checks, totaling about $650,843, that Wood had deposited into her own account. (Source)

Former Property Manager Sentenced To Prison For Embezzling $70,000+ From Federally Subsidized Housing Complexes Over 9 Years - November 4, 2021

Alicia Gardner was employed by Garden Homes Management Corporation with responsibilities that included managing housing complexes in Brooklyn, Connecticut, and the St. Mary's housing complex in East Hartford. The housing complexes principally catered to elderly and disabled citizens receiving federal rental subsidies from the U.S. Department of Housing and Urban Development or the U.S. Department of Agriculture.

Between approximately 2009 and 2018, Gardner diverted rental payments and other tenant fees to a separate account she had set up for cable fees, and then diverted those payments to pay more than $400,000 in personal expenses. Gardner also overcharged tenants a total of more than $60,000 for cable expenses, which increased the amount of money available to be diverted. In addition, Gardner embezzled at least $70,000 in rental payments paid by St. Mary's tenants. (Source)

Former Office Manager Sentenced To Prison Embezzling $2.7 Million+ From Employer For Personal Use / Gambling - November 3, 2021

Melissa Dihel began stealing from her employer less than two years after pleading guilty to embezzling from another business, for which she received a deferred sentence on Dec. 16, 2009, in Tulsa County District Court.

Dihel embezzled more than $2.7 million from her employer from 2011 until May 2019. Dihel took advantage of her trusted position as an office manager at the business and forged the president's signature on approximately 334 checks for her own benefit and to the detriment of the company. She made some checks payable to herself, some to her boyfriend and a family member, and some to personal credit card companies to pay her monthly credit card bills. Her boyfriend and family member were unaware of her scheme. Dihel further manipulated accounting entries in her employer's books and records to cover her tracks. Dihel stated in her plea agreement that she spent most of the money on gambling. (Source)

Former Accountant For Non-Profit Organization Sentenced To Prison For Embezzling $2 Million+ Over 8 years - November 3, 2021

From as early as 2012 and continuing through June 2020, Angelia Brown embezzled more than $2 million from her former employer, a non-profit organization that focuses on the welfare of abused children. Brown worked as a staff accountant for the nonprofit organization.

Brown forged company checks and deposited them into her personal bank account. Brown also concealed the fraud scheme from her former employer by altering the checks after they had been deposited into her bank account. Brown forged 885 checks that were drawn on her former employer's bank accounts, causing a total loss amount to her former employer of $2,064,464.99. (Source)

Former School Bookkeeper Sentenced To Prison For Embezzling $121,000+ - November 2, 2021

Carlina Moore was employed by the Montessori Educational Center, Inc. (MEC) as a bookkeeper from May 2018 to August 2020 and she handled all in-house bookkeeping for them.

On or about August 25, 2020, the MEC's administrator reviewed their bank account and discovered a questionable transaction. This prompted the administrator to conduct a further review of the bank and credit card accounts. Their investigation into the questionable transaction revealed that Moore was embezzling funds from the MEC's accounts without their knowledge or authorization.

Law enforcement agents further investigated the fraudulent activity and confirmed that Moore had in fact defrauded the MEC by transmitting funds by way of wire communications in interstate commerce. Moore admitted that she devised a scheme to defraud the MEC and that she did so in order to obtain money and property from the MEC fraudulently and for her own personal gain. She admitted that she embezzled $121,600.50 from the MEC. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Fraudster Paid 7 Amazon Employees A Total Of $160,000 To Help Him Hijack Sellers' Accounts And Products - November 18, 2021

The fraudster known as Krasr paid off 7 employees inside of Amazon to help him hijack other sellers' accounts and copy their products, according to company documents.

The Amazon employees leaked customer data and product information while blocking and reinstating sellers at Krasr's request,

Krasr recruited the employees over LinkedIn and Facebook. The 7 Amazon employees were paid a total of $160,000 over several years. Upon discovery, Amazon fired the 7 employee who were caught working with the Krasr.

But this wasn't the only time Amazon located moles within the company. 2 Amazon employees in China were involved in bribes and selling personal data a new report revealed. (Source)

Pharmacy Owners, Physicians, Pharmacists, Patient Recruiters Plead Guilty In $126 Million Fraud Scheme Involving Department of Labor Office of Workers' Compensation Programs And TRICARE - October 27, 2021

The defendants submitted false and fraudulent claims to the OWCP and TRICARE for prescriptions for compounded and other drugs prescribed to injured federal workers and members of the armed forces. The defendants also paid kickbacks to patient recruiters and to physicians to induce them to prescribe these drugs. The defendants chose the particular compounds and other drugs based not on the patients' medical needs but in light of the amount of reimbursement for the drugs. The drugs were then mailed to patients, even though the patients often never requested, wanted, or needed them. (Source)

2 Owners & 18 Employees Of Physical Therapy Practice Charged With Fraud Over 14 Years - November 9, 2021

From January 2007 to October 2021 to commit wire fraud and health care fraud. The multi-faceted conspiracy had numerous components including:

A physical therapy practice in Erie County, Pennsylvania, and 20 people, 18 of them who were employees have been charged by a federal grand jury of conspiracy to commit wire and health care fraud. (Source)

Mayor Of Stonecrest Georgia & Bookkeeper Arraigned On Federal Charges For Theft Of COVID-19 Relief Funds - November 10, 2021

Jason Lary, the Mayor of Stonecrest, Georgia, has been arraigned on federal charges of wire fraud, conspiracy, and federal program theft. The charges relate to a scheme to allegedly steal federal relief funds granted to Stonecrest to address the economic fallout of the COVID-19 pandemic.

Lania Boone, a bookkeeper for the entity hired by Stonecrest to disburse the relief funds, has also been arraigned on a federal charge of conspiring with Lary to steal relief funds.

Under the CARES Act, the federal government distributed COVID-19 relief funds to individual Americans, federal agencies, and state and local governments, including $125 million to DeKalb County. The federal government permitted DeKalb County to further disburse these relief funds to its municipalities. In July 2020, the DeKalb County Board of Commissioners voted to disburse some of the relief funds to its municipalities, including a $6.2 million grant to Stonecrest.

Stonecrest did not disburse the $6 million allocated to the Stonecrest Cares Program and Small Business Program. Instead, the city contracted with Municipal Resource Partners Corporation, Inc. ("MRPC") to provide accounting services and to disburse the relief funds as directed by Stonecrest. Before the contract was signed, Lary allegedly worked behind the scenes to assist MRPC, including by recruiting its CEO, opening its bank accounts, and ensuring that Lania Boone would be hired as MRPC's bookkeeper.

From about November 2020, until in or about February 2021, Lania Boone signed dozens of checks on behalf of MRPC, directing millions of dollars of relief funds to individuals, businesses, churches, and non-profit organizations. Lary allegedly helped decide where the relief funds were directed. (Source)

THEFT / DESTRUCTION OF COMPANY PROPERTY

Former Employee Of Firearms Dealer Steals 335 Firearms - November 3, 2021

Brandon Parker was employed by Master Pawn of Horse Cave, a federally licensed firearms dealer, located in Horse Cave, Kentucky.

Parker admitted that he stole approximately 335 firearms from Master Pawn between November 2016 and August 22, 2018. Parker also admitted that he provided false information on ATF Forms 4473 by entering identification information of legitimate purchasers, without their knowledge, to fraudulently obtain and steal the firearms. (Source)

FedEx Driver Dumped Hundreds Of Packages Into Ravine On 6 Different Occasions - November 30, 2021

Authorities in Alabama said they are investigating the hundreds of FedEx packages found in a ravine after being reported missing and have questioned the driver they think is responsible.
The driver is no longer providing service on behalf of FedEx Ground, FedEx said in a statement.

Mark Moon, the Blount County sheriff investigating the FedEx dump found last week, said a driver must have intentionally dropped hundreds of packages in the ravine six different times in a case that spans 450 customers. Residents discovered the lost packages.(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)

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 (**3,100+ 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