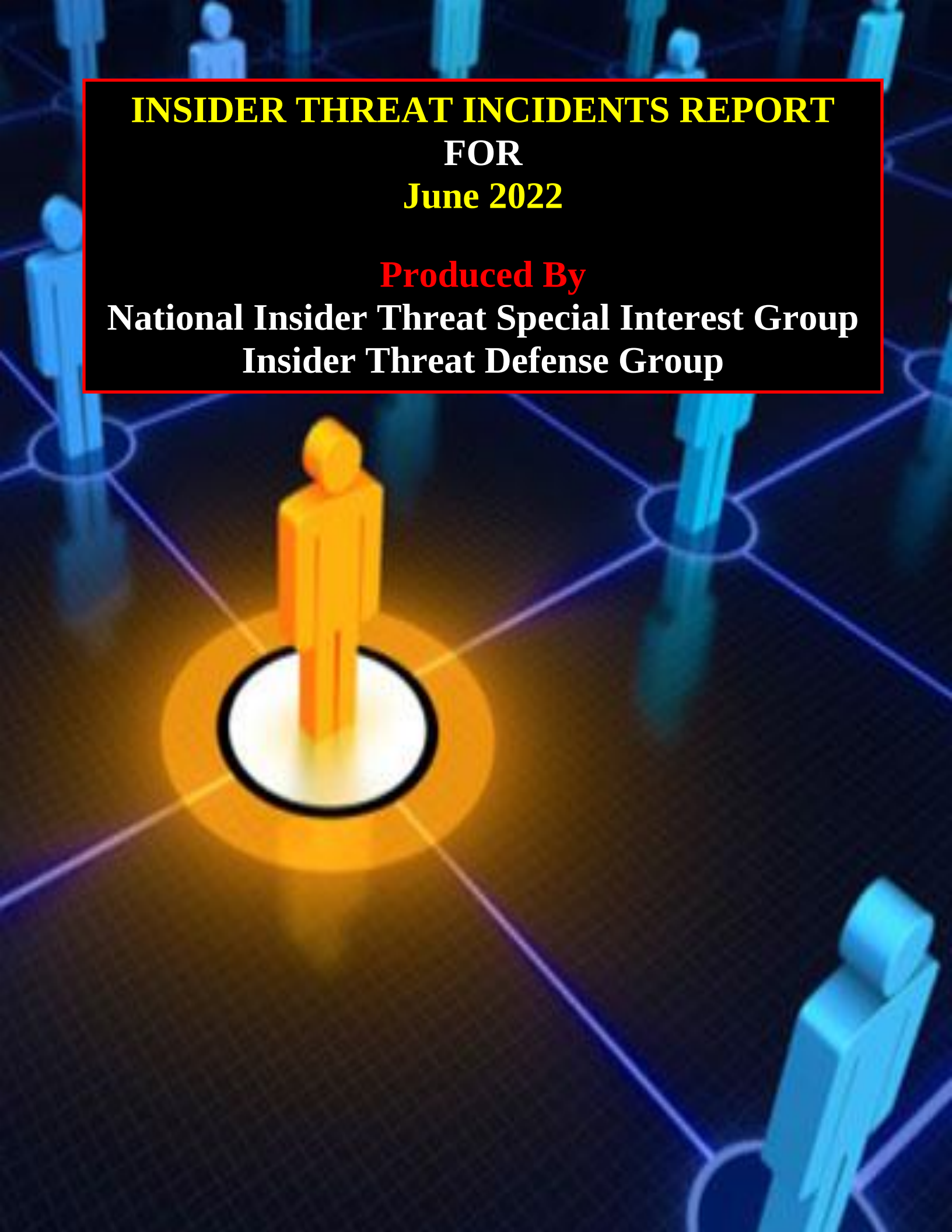

INSIDER THREAT INCIDENTS REPORT
FOR
June 2022

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 **3,800+** 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 22 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 JUNE 2022

U.S. GOVERNMENT

Former General Services Administration (GSA) Contracting Official Pleads Guilty To Accepting $411,000+ In Bribes For Contract Awards - June 17, 2022

Beginning in approximately December of 2015 and continuing through August 2019, Charles Jones, a GSA employee, accepted bribes from government contractors in return for awarding federal contracts to Contractors USA and SDC Contracting LLC.

Jones was employed as a Supervisory Construction Control Representative with the GSA. He had responsibility for the management and oversight of construction and renovation projects at certain federal buildings throughout the Norfolk, Richmond, and Alexandria areas. Jones received bribes totally $411,192.00 from the President of Contractors USA Inc., in exchange for awarding them federal construction projects. In October of 2019, Jones received a cash payment from the President of SDC Contracting LLC in exchange for awarding a contract valued at approximately $1,369,501.00. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

4 Navy Officers Convicted Of Bribery In Very Large Scandal Involving 33 Others - June 29, 2022

Former U.S. Navy Captains David Newland, James Dolan and David Lausman and former Commander Mario Herrera, all of whom once served in the Navy's Seventh Fleet, were convicted for accepting bribes from foreign defense contractor Leonard Francis.

9 members of the U.S. Navy's Seventh Fleet, including the 4 defendants convicted today, were indicted by a federal grand jury in March 2017.

This long-running fraud and bribery investigation has resulted in federal criminal charges against 34 U.S. Navy officials, defense contractors and the GDMA corporation. 29 previously pleaded guilty. With today's four convictions, 33 defendants have now been convicted of various fraud and corruption offenses. (Source)

Former U.S. Military Pilot Admits To Acting As Paid Agent Of China and Lying on National Security Background Forms - June 23, 2022

Shapour Moinian served in the Army in the United States, Germany, and South Korea from approximately 1977 through 2000. After his service, Moinian worked for various cleared defense contractors in the United States.

While Moinian was working for a cleared defense contractor, on various aviation projects used by the U.S. military and U.S. intelligence agencies, he was contacted by an individual in China who claimed to be working for a technical recruiting company. This person offered Moinian the opportunity to consult for the aviation industry in China.

Moinian admitted to being an unregistered agent of a foreign power, lying on his background check paperwork to obtain his security clearance, knowingly providing proprietary information to people controlled by the Chinese government, and willingly receiving payments from them. (Source)

USS Michigan Sailor Tried To Distribute Cocaine In Sub's Missile Compartment - June 23, 2002

As part of a drug investigation aboard the USS Michigan, a sailor standing watch in the submarine's missile compartment was accused of trying to distribute cocaine to another sailor.

The revelation of drug distribution inside the submarine comes after a 2019 incident where an officer on the USS Michigan was accused of selling cocaine in Seattle, and the 2020 fentanyl overdose death of a sailor while aboard the USS Carl Vinson, which had been docked at the Puget Sound Naval Shipyard.

In the recent case of drug-dealing and use aboard the USS Michigan, two sailors confessed to buying cocaine from Chase Brown, according to a Naval Criminal Investigative Service report.

The sailor told the NCIS agent since January he bought about two grams of cocaine biweekly from Brown. (Source)

Former NCIS Agent Convicted Of Corruption & Releasing Classified Information To Foreigner - June 17, 2022

A former Naval Criminal Investigative Service (NCIS) special agent was convicted of corruption elated offenses stemming from her relationship with the subject of a multi-agency counterterrorism investigation.

Leatrice Daniels was convicted in the Southern District of Texas of obstructing justice, making false statements, and accepting money and gifts for official acts.

Daniels was a veteran NCIS special agent working in Dubai, United Arab Emirates. There, she met Nadal Diya, a Syrian businessman living in Dubai looking for help in securing a visa to the United States. At that time, Diya was the target of several federal investigations.

The jury heard from 16 government witnesses, which included numerous agents and Diya himself. Testimony revealed that in 2017, Daniels used her position to get certain benefits from Diya in exchange for providing information to him about his visa status. The gifts included an expensive birthday party at Diya's home, approximately $1,400 in cash, and the promise of a job for her son in Diya's company.

In late December 2017, federal agents questioned Daniels about Diya. However, she failed to disclose her intimate relationship with him, the gifts he had given her, the job he offered her son, and the classified information she provided.

Several months later in May 2018, she left Dubai for Hawai'i for a highly sensitive and coveted job. However, she soon learned she would not get the new position. It was only then she confessed to superiors and investigators about her illicit relationship, the monies, party, and gifts she had received and the classified information she had previously revealed. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

2 California State Political Leaders Resign After FBI Agents Accuse Them Of Bribery & Fraud In Connection With The City's $320 Million Sale Of Stadium - May 23, 2022

2 prominent Orange County political leaders resigned within 24 hours of each other amid fallout from a sprawling federal public corruption investigation linked to the proposed sale of Angel Stadium and allegations that a secretive "cabal" controlled Anaheim's politics.

Anaheim Mayor Harry Sidhu announced he was stepping down after being accused of bribery, fraud, obstruction of justice and witness tampering in an affidavit supporting a search warrant application earlier this month.

The FBI affidavit states that Sidhu gave Major League Baseball's Angels confidential information on at least two occasions during the city's negotiations with the team over the $320 Million Angel Stadium sale, and hoped to get a million-dollar campaign donation from the team. (Source)

Former Deputy Clerk Of Court Sentenced To Prison For Role In $1.3 Million+ Fraud Scheme Involving 5 Co-Conspirators - June 2, 2022

Willie Demps is the former Deputy Clerk of Court for Muscogee County, Georgia.

Demps worked for the court for approximately 30 years and supervised money deposits received by the clerk's office. The Clerk's Office received money from fines and condemnations, and payments were frequently made in cash.

From at least 2010 to 2019, Demps maintained a safe in his office to store sums of cash that were collected by the Clerk's Office. During the business day, this safe was rarely locked, even when Demps was away from his office. Demps was responsible for depositing cash received by the Clerk's Office into an appropriate Clerk of Superior Court bank account. Records indicate that the Clerk's Office received over $5.5 million in cash during the period of 2010-2019, yet only a single cash deposit of approximately $210 was made into official accounts in 2019. No cash deposits were made in other years.

From Oct. 2010, to Nov. 2019, Demps issued at least 330 Clerk of Superior Court checks payable to the named the 5 co-conspirators, totaling at least $1.3 million.

Demps would meet various co-conspirators in locations away from his place of business at the clerk's office to give the illicit checks to them to be cashed at banks. The co-conspirators
cashed the checks and returned the money to Demps, who would give the participating co-conspirators a portion of the money. Demps admits he used the money for personal expenses, to send money to foreign countries and to spend at casinos. (Source)

Technology Director For School Sentenced To Prison For Stealing $500,000+ Over 9 Years For Personal Use - June 29, 2022

Todd Wessels was the Curriculum and Technology Director for a private, religious, not-for-profit school district in Dubuque. 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 sometime prior to June 2011, and continuing into early 2020, 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, Inc.

Wessels also sold the school district's computer equipment on third-party Internet websites without its knowledge or permission.

Wessels admitted he stole over $500,000 as a part of his scheme. Due to a lack of a written inventory and lack of records before 2011, however, the full extent of his scheme remains unknown. The school district hired Wessels in 2001, and he was one of its highest paid employees, earning nearly $100,000 at the time the scheme was discovered. During the time that Wessels was perpetuating his scheme against the school district, the school district was experiencing financial difficulties and closing a number of schools as a result.

Wessels had made hundreds of purchases for food, hotel stays and other travel-related expenses for himself and his family, tickets to off-Broadway shows, new pools each year, and expensive electronics such as a virtual reality headset, robots, and Apple televisions. (Source)

Former To North Carolina Town Finance Director Arrested On Charges For Embezzling $500,000+ - June 10, 2022

Gay Tucker embezzled more than $500,000 from the Town of Spring Lake during her tenure as Finance Director and Accounting Technician for the Town. Tucker carried out the embezzlement through fraudulent checks containing forged signatures of the Mayor and Town Manager. (Source)

City Employee Admits Role In Scheme To Steal $636,000+ Of COVID Relief Funds - June 14, 2022

John Bernardo was employed by the City of West Haven Connecticut as a Housing Specialist in the office of Community Development Administration.

In January 2021, Bernardo and another city employee 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. Bernardo received a portion of these funds. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Police Chief Sentenced To Prison For Illegally Trafficking 200 Fully Automatic Machine Guns - June 2, 2022

Former State Highway Patrol Officer Sentenced For Selling Firearms Without a License, With Help Of Convicted Felon - June 2, 2022

In January 2021, the Federal Bureau of Investigation (FBI) learned that Timothy Norman was selling firearms to various persons, including a convicted felon, while employed as a North Carolina State Highway Patrol (NCSHP) trooper.

During the investigation, the FBI learned that Norman used a convicted felon as a middleman for various firearms, which included decommissioned NCSHP service weapons: Sig Sauer P226 .357 semi-automatic pistols, Arma Lite, AR-15 5.56mm semi-automatic rifles, and Beretta, Model 1201FP, 12-gauge shotguns. Thereafter, law enforcement agencies conducted three successful controlled purchase operations.

On July 7, 2021, investigating agencies executed a search warrant on Norman's home and seized thousands of rounds of ammunition and over fifty firearms. In Norman's patrol car, they found two more firearms (neither of which was NCSHP-issued), including one AR-15 rifle that Norman purchased from the FFL earlier that year. There was also an envelope with over $2,000 in cash, which included FBI buy money from one of the controlled buy operations referenced above. (Source)

OTHER RELATED INCIDENTS

- Former Ohio Police Chief Plead Guilty In Role To Illegally Traffic 200 Fully Automatic Machine Guns - April 18, 2022
- Police Officer Indicted For Theft Of 54 Firearms / Ammunition From Police Weapons Vault - January 20, 2021
- Former Southwest Airlines Employee Sentenced To Prison For Stealing Firearms From Luggage - November 30, 2021
- Active Duty Sailor And His Former Navy Colleague Are Charged With Conspiring To Traffic Guns - August 31, 2021
- Former Army Soldier Sentenced To Prison For Burglarizing Firearms Dealers - September 29, 2020
- Former Hospital Director Of Security Pleads Guilty To Buying Firearms With Hospital Funds And Then Selling Guns For Profit - June 17, 2020

Former Police Chief Sentenced To Prison For Illegally Trafficking 200 Fully Automatic Machine Guns - June 2, 2022

Dorian LaCourse is the former Chief of Police in the Village of Addyston, Ohio. 2 federally licensed firearms dealers in Indiana were his coconspirators, Johnathan Marcum and Christopher Petty.

LaCourse, Marcum, and Petty, illegally exploited a law enforcement exception to the federal ban on the possession or transfer of fully automatic machine guns. As Chief of Police, LaCourse signed multiple demonstration letters falsely stating that the Village of Addyston Police Department was interested in purchasing various types of machine guns, including military-grade weapons, and asking that Marcum and or Petty give the demonstration. Marcum and Petty then sent the letters to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to obtain the weapons. Addyston is a village in southwestern Ohio of approximately 1,000 residents. LaCourse was the village's only full-time police officer.

LaCourse also placed direct orders for German-made machine guns that were purported to be paid for by the Police Department. In fact, the purchases were fully funded by Marcum and Petty and intended to bypass restrictions on the importation of such weapons by anyone other than the police or the military.

The Addyston Police Department was never authorized to purchase any of the machine guns, and the Indiana gun dealers never provided any demonstrations of machine guns to the police department. Instead, the gun dealers resold the machine guns at a significant profit. In some instances, a gun dealer resold illegally acquired machine guns for five or six times the purchase price. The conspirators purchased or caused the importation of approximately 200 fully automatic machine guns. LaCourse received over $11,500 from the gun dealers for his role in the scheme. (Source)

Police Officer And His Wife Charged For $99,000 Fraud Scheme Against Fraternal Order of Police For Spending On Personal Items - May 31, 2022

Michael Hardin, an officer with the St. Joseph Police Department, was the president of the Fraternal Order of Police Northwest Missouri Lodge for approximately 10 years.

Sarah Hardin, formerly a deputy with the Buchanan County Sheriff's Department, was the treasurer of the lodge for approximately 10 years.

The Hardins used debit cards linked to the bank accounts of the Fraternal Order of Police Northwest Missouri Lodge to make $99,000 in purchases for their own personal gain over a 4 year period from December 2015 to December 2019.

Sarah Hardin used two debit cards to make purchases at Walmart, Menards, Party City, HyVee, and other businesses for personal items and expenses. Michael Hardin allegedly used one debit card to make purchases from various merchants, including Hampton Inn, for personal items and expenses. (Source)

Former Detroit Police Department Officer Sentenced To Prison For Taking $3,200 In Cash Bribes - June 14, 2022

Alonzo Jones was sentenced to 15 months in prison and 2 years of supervised release based on his plea of guilty to accepting bribes.

Jones, an officer with the Detroit Police Department for over 30 years, corruptly accepted cash bribes on five separate occasions, totaling $3,200, with the intent to be influenced and rewarded in connection with his duties overseeing and running the Detroit Police Vehicle Auction. The last bribe he took was right before he retired from DPD in May 2021. (Source)

Police Officer Charged With COVID Relief Fraud - Used Loan Money To Service & Repair His Vintage Car - June 16, 2022

Jason Carter was a Coral Springs Florida Police Officer who fraudulently applied to the U.S. Small Business Administration (SBA) for a COVID-19 relief advance grant and low-interest loan.

Carter submitted a fraudulent Economic Injury Disaster Loan (EIDL) application and loan agreement on behalf of Jason S. Carter, Inc., a South Florida business he allegedly owned and operated. That application falsely and fraudulently certified, among other things, that during the twelve 12 months prior to January 31, 2020, the business had gross revenues of $100,000. In reality, the business had only minimal gross revenues during that period. Carter fraudulently certified that he would use the funds only for business expenses to alleviate economic injury that the COVID-19 pandemic caused to the business. Carter spent more than $21,000 of the SBA loan money at a car repair and detailing company for luxury vehicles and high-end auto parts. (Source)

Former Federal Probation Officer Pleads Guilty To Extorting Individuals Under Her Supervision For Personal Gain - June 14, 2022

Form 2016 through 2018, Helwa Qasem accepted Xanax, cash, a sweater, a bag and below-market personal services in exchange for official actions as a probation officer.

During her time as a probation officer, she accepted cash, pills, goods and services from individuals under her supervision. (Source)

Prison Guard Charged With Accepting $4,300+ In Bribes To Allow Inmate To Receive Smuggled Items - June 27, 2022

Tiffany Fletcher is a Corrections Officer and Counselor at the privately operated McRae Correctional Facility.

Tiffany Fletcher is accused of accepting five cash bribes totaling $4,390 from June to December 2019, and in return acted in violation of her official duties as a correctional officer by failing to report or investigate prohibited objects being brought into McCrae Correctional Facility. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Bank Teller Sentenced To Prison For $144,000 Of Bank Fraud - June 13, 202

Ana Amesquita was the head teller at the Inwood branch of City National Bank.

In June 2019, Amesquita began a scheme to process ATM deposits without the supervision of a second bank employee, violating the bank's policy. She would then take some of the cash for her own personal use and misrepresent the facts in the general ledger. (Source)

Amesquita was also ordered to pay $144,661 in restitution to the bank. (Source)

Former Bank Branch Manager Sentenced To Prison For Loan Fraud Scheme - June 30, 2022

Gabe Outtrim was the Branch Manager and Vice President of the CorTrust Bank branch in Leola, South Dakota,

Beginning on approximately September 17, 2018, and continuing through February 21, 2019, Outtrim had lending authority to approve loans up to $200,000 without having to send the loan application and supporting documentation to the bank's loan committee for review and approval.

Outtrim made a nominee loan in the name of an unknowing bank customer and used the loan proceeds for his own benefit. (Source)

TRADE UNIONS

Former Police Union Treasurer Sentenced To Prison For For Stealing $50,000 Of Union Funds To Pay For Vacations - June 27, 2022

Joshua Fernandes abused his position as Union Treasurer by using nearly $50,000 in union funds to pay for personal expenses including vacations, family outings, and a monthly wireless family phone plan, among other things. Fernandes carried out his scheme by reimbursing his personal credit card accounts with union funds and by using the union's credit cards to pay directly for non-union expenses. (Source)

Former Union Benefit Plan Administrator Admits Embezzling $140,000 - June 3, 2022

George Laufenberg was the Administrative Manager of the Northeast Carpenters Pension Fund. Laufenberg was a fiduciary and participant in the pension fund.

He admitted stealing $140,000 that was paid to him under a deferred compensation agreement to which he was not entitled. (Source)

TSA Labor Union President Pleads Guilty To Misappropriating $3,000 Of Union Funds For Personal Travel - June 2, 2022

Marie LeClair was the president of the American Federation of Government Employees, Local 2617, which was based in Boston and represented TSA employees.

Beginning in or about March 2015, LeClair engaged in a scheme to defraud the union by misappropriating funds belonging to the union for her personal use.

LeClair transferred funds from union accounts to a travel debit card issued in her own name without the knowledge or authorization of the union and used the misappropriated union funds for personal expenses. On May 22, 2018, LeClair made a wire transfer of $3,000 from a union account to her personal travel debit card. (Source)

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

Scott Rodgers embezzled a total of $80,756. From 2016, when he became president of Postal Mail Handlers Local 314, to April 2020.

Rodgers made four unauthorized ATM withdrawals from the union account and used the union debit card for personal purchases including meals, fuel, transportation, shopping and travel. He also falsely claimed and received "lost time" payments, or compensation for wages lost when performing work for the union. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Employee Convicted Of Stealing Microchip Trade Secret For Company He Started - May 28, 2022

Haoyang Yu was convicted of possessing the prototype design of a microchip, known as the HMC1022A, which was owned and developed by Analog Devices, Inc. (ADI), a semiconductor company.

From 2014 to 2017, Yu worked at ADI, where he designed microchips used by the communications, defense and aerospace industries. As a result of his work, Yu had access to ADI's present and future microchip designs, including their schematic files, design layout files and manufacturing files.

While he was an ADI employee, Yu started his own microchip design firm, Tricon MMIC, LLC, and used the stolen HMC1022A design to manufacture a knock-off version of ADI's chip. Yu began selling his version of HMC1022A prior to ADI's release of its chip. ADI cooperated fully in the government's investigation. (Source)

Former Employee Sentenced To Prison For Identity Theft To Create Fraudulent Tax Returns To Obtain $77,000+ Of Refunds - June 16, 2022

From February 1999 through August 2015,Tamara Manuel worked at Sonoma Development Center (SDC), which was a large, state-run facility serving the needs of individuals with developmental disabilities. In her role at SDC, Manuel had access to SDC patients' personal identification information, including Social Security Numbers and birthdates.

Manuel began stealing SDC patients' identities in 2011 and filing fraudulent tax returns in their names. In the returns, Manuel falsified, among other things, the purported taxpayers' employment, wages, tax withholdings, and dependents. She did so to claim exemptions, tax credits, and refunds the purported taxpayers were not due. For example, Manuel falsely represented in a tax return that an SDC patient made over $23,000 in annual income as a forklift driver, had a dependent, and was owed a child tax credit. In reality, the patient had no income or dependents and was severely disabled, requiring observation and care 24 hours a day.

In total, Manuel stole the identities of at least 18 SDC patients to file 33 fraudulent tax returns in which she claimed refunds totaling over $77,000. Manuel obtained almost $50,000 in refunds from the Internal Revenue Service. (Source)

Taco Bell Employee Accused Of Taking Pictures Of Credit Card To Buy Personal Items - June 22, 2022
Laquawanda Hawkins worked at a South Carolina Taco Bell is accused of taking photos of customers' credit cards and using the numbers to buy items for herself.

Restaurant surveillance video taken showed Hawkins taking photos of credit cards with her phone before returning them to drive-thru customers.

During June, at least four customers who visited the Taco Bell contacted the police department complaining of fraudulent charges to their debit or credit cards.

Hawkins used the stolen credit card information for purchasing pizza, scooter rentals and purchases at Advance Auto, bought shoes and a cell phone online. (Source)

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

Nurse Practitioner Pleads Guilty To Conspiracy In $15 Million Durable Medical Equipment Kickback Scheme - June 30, 2022
During 2018 and 2019, Justin Segrest was a nurse practitioner and was working for a telemedicine company based in Delaware.

Between 2018 and 2019, Segrest caused thousands of claims to be submitted to Medicare for medically unnecessary orthopedic braces and other durable medical equipment (DME).
Segrest facilitated the scheme by making false claims in medical records to support the fraudulent claims. He did so by signing false medical records describing purported assessments of Medicare beneficiaries and certifying that he had performed corresponding medical examinations when, in fact, Segrest had no interaction with the beneficiaries and made no medical determination whether the devices were medically necessary or the beneficiaries needed the DME.

Segrest received from the telemedicine company unsigned orders for orthopedic braces for the beneficiaries, which he signed and returned to the telemedicine company in exchange for $15 for each purported assessment that he performed. Through this scheme, Segrest caused the submission of nearly $15 million in false and fraudulent claims to Medicare. (Source)

Former Office Manager Sentenced To Prison For Stealing Opioids From Veterinary Office For Personal Use - June 17, 2022
In late 2018 and 2019, federal investigators noted that an unusually large amount of hydrocodone had been ordered by the veterinary office. In June 2019, the investigators conducted an audit at the animal hospital during which Melissa Paradise was identified as the Office Manager responsible for record keeping regarding prescriptions.

Paradise admitted to investigators that she used the DEA registration number assigned to a veterinarian in the practice without the veterinarian's knowledge or consent to order controlled substances which she then stole for her personal use. Paradise also admitted that she forged the signature of a second veterinarian on other prescription documents and diverted those drugs for her own use. (Source)

Veteran Affairs Hospital Nurse Pleads Guilty To Stealing COVID19 Vaccination Cards & Selling Them On Facebook - June 17, 2022

Bethann Kierczak was a registered nurse with the Veteran's Hospital in Detroit.

Kierczak admitted to stealing or embezzling authentic Covid-19 Vaccination Record Cards from the VA hospital, along with vaccine lot numbers necessary to make the cards appear legitimate. She then resold those cards and information to individuals within the metro Detroit community. Kierczak's theft of Covid-19 Vaccination Record Cards began at least as early as May 2021 and continued through September 2021. Kierczak sold the cards for $150-$200 each and communicated with buyers primarily via Facebook Messenger. (Source)

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

Former Bookkeeper Sentenced To Over 4 Years For Stealing $2.6 Million / Used Fund For Personal Expenses, Gambling, Luxury Vacations - June 28, 2022

Angela Sabatine pleaded guilty to charges of wire fraud, aggravated identity theft and bank fraud in connection with a scheme to create false financial records for the non-profit and then steal the funds for her personal use.

Sabatine was a Accounting Administrator for the Delaware River Waterfront Corporation (DRWC), an organization whose mission is to design, develop, and manage the central Delaware River waterfront from Oregon to Allegheny Avenues for the benefit of Philadelphia residents.

DiPietro-Sabatine used the non-profit's computerized accounting software to create false expense items for legitimate vendors of DRWC in order to invoice services that were never rendered. Sabatine generated DRWC checks for these false expense items, manipulated the computerized accounting software to change the payee on the check from the legitimate vendor to herself, and forged the signatures of DRWC's authorized signatories, the President and Vice President, on these unauthorized checks made payable to herself. She spent the stolen proceeds, more than $2.6 million, on personal expenses, including gambling and luxury vacations. (Source)

Former Bookkeeper Pleads Guilty To Embezzling $3 Million+ From Employer Over 5 Years To Pay For Travel & Investments - May 27, 2022

Mancy Martin admitted to defrauding her employers, Mid-Kansas Wound Specialists and Emergency Services P.A. Martin worked for the companies as a Bookkeeper, Business Manager and Chief Operating Officer.

An audit revealed that from 2012 to 2017, Martin embezzled approximately $3.1 million by fraudulently obtaining money from her employers' banks, She used funds to pay for personal expenses, travel, and investments then made false accounting entries to disguise the embezzlement as payments or transferred funds between entities. (Source)

Former Property Management Company Employee Admits To Stealing $2.67 Million In Rent Checks For Personal Use - June 15, 2022

Loria Anderson worked in the property management office of an apartment building in Philadelphia, Pennsylvania. Tenants paid their rent and other expenses to the property management office.

From January 2011 to October 2018, Anderson stole 697 checks and money orders totaling $2.67 million her employer, drove them from Philadelphia to New Jersey, and deposited those checks and money orders into a nominee bank account that she opened using a fake Social Security number. Anderson admitted that she used the money to pay personal expenses. (Source)

Former Car Dealer Bookkeeper Sentenced To Prison For Stealing $2 Millon Over 8 Years To Fund Her Gambling Addiction - May 3, 2022

A long-term accountant for a car dealer who stole almost $2 million from the company to fund her gambling addiction.

Sandra Balfour pleaded guilty and admitted to unlawfully transferring funds from Brisbane Motor Auctions and Platinum Vehicle Sales to her own personal bank account between 2010 and 2018.

Balfour had been working as a bookkeeper for more than 20 years and was a trusted employee who had access to the company's accounts and payment system.

To avoid detection, Balfour used another employee's log in information to generate the payments, and then used her own details to authorize them. (Source)

Paralegal Pleads Guilty To Embezzling $1.2 Million+ From Law Firm Trust Account - June 1, 2022

From at September 2015, through December 2017, Lindsey Passmore, was a paralegal at a Richmond area law firm that specialized in real estate law. That firm held loan proceeds in an escrow account for a private lender, Joshua Romano. Romano was involved with the purchase, rehabilitation, and sale of homes around Richmond. The loan proceeds were earmarked for Romano to use them only for the purchase of purchase and rehabilitation of specific properties, and only with the lender's express approval for each disbursement. In order to cover this up, Passmore sent the lender emails that falsely reported the balances held in escrow for these properties.

Passmore disbursed a total of $1,206,953.27 of the lender's funds held in escrow for Romano's projects without receiving the lender's approval or by misleading the lender about how the funds were to be used. The funds were then allegedly used by Romano for purposes outside the scope of the agreements with the lender. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $881,000 From Employer - June 22, 2022

In 2014, Kimberly Janovec became the Director of Operations for MI5, Inc., a Denny's franchisee that owned and operated eight Denny's franchises in Minnesota and Wisconsin.
Janovec had extensive managerial oversight for all eight restaurants, including payroll, cash deposits, vendor and contractor billing, marketing, and coordinating reimbursements from Denny's Corporate.

From April 2014 through July 2019, Janovec used her position to embezzle funds from MI5 and Denny's Corporate by generating and submitting false requests for vendor payments and then diverting those payments for her own use and benefit. Peterson-Janovec also manipulated the company's payroll system to issue herself unauthorized compensation using the names of employees who no longer worked for the company.

As part of the scheme, Peterson-Janovec falsified records, created fake email accounts, and generated fake email traffic in which she impersonated employees of various purported vendors. Janovec received approximately $336,000 in bogus vendor payments and approximately $20,000 in fraudulently issued payroll submissions using the identities of other people. Janovec was also responsible for stealing an additional $181,000 in cash deposits from MI5. (Source)

Former Financial Officer Pleads Guilty To $800,000+ Of Wire Fraud - June 30, 2022

Betweeen 2013 and 2020, Rodney Ellis while employed by Sumter Behavioral Health Services (SBHS), as its Financial Officer, defrauded the non-profit out of at least $800,000 by diverting funds from SBHS banking accounts to his own personal banking accounts to which he was not entitled. (Source)

Former Employee Sentenced To Prison For Embezzling $795,000+ From Employer - June 3, 2022

From in or about April 2017 through June 2019, Kayla Figelski stole at least $796,747 from her employer, an elder law attorney, in Malden.

Figelski perpetrated the scheme by forging checks to herself from her employer's checking accounts, including conservatorship, trust and estate administration accounts her employer maintained for the firm's elderly clients and their estates.

Figelski deposited the checks into her own bank account, from which she withdrew the funds, or directly cashed the checks. Figelski concealed the scheme by altering bank statements to make it appear that the checks were written to legitimate vendors. (Source)

Former Office Manager Sentenced To Prison For Embezzling $775,000+ From Employer Over 6 Years - June 13, 2022

Cynthia Jones was the Office Manager for a Central Texas business. In that role, she had access to the company's accounting system and checkbook.

From 2012 to 2018, she forged over 70 company checks and stole over $775,000. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $600,000+ From Employer To Pay For Her Persoanl Credit Card Expenses - June 9, 2022

In 2013, M&D Construction hired Nicole Lopez as a Bookkeeper / Accountant for the business. As part of her duties, Lopez was given access to M&D's bank account and was given administrator permission over M&D's Quick Books account.

Between January 2017 and January 2020, Lopez charged over $600,000 on her personal credit card accounts. Her expenses focused mostly on consumer shopping and travel, and included over $80,000 on purchases from Amazon, over $115,000 on general retail purchases, over $46,000 on clothing, over $57,000 on travel, over $34,000 on restaurants, over $24,000 on beauty products, over $12,000 on furniture, and over $7,000 on plastic surgery. None of these purchases was related to M&D's business operations.

To pay for her personal credit card expenses, Lopez embarked on a scheme to embezzle money from M&D by using her access to M&D's bank account to direct payments from the M&D business account to her personal credit accounts without the knowledge of or authorization from M&D's owners.

Between January 2017 and January 2020, Lopez directed 72 payments from M&D to her personal credit accounts and embezzled approximately $632,362.65. (Source)

IT Technology Manager Pleads Guilty To Embezzling $360,000+ From Non-Profit Organization For Personal Expenses - June 22, 2022

From April 2015 to May 2020, Rick Kapiris worked as the Information Technology Manager at a non-profit organization.

As part of his responsibilities, the organization provided Kapiris access to two company credit cards to purchase equipment and services as needed. Beginning in 2016, Kapiris used the two company credit cards to purportedly purchase equipment from two vendor accounts on the web app Square and one account on Amazon. In reality, Kapiris created the three vendor accounts to embezzle the funds and fabricated sales invoices for purportedly purchased equipment to conceal the scheme. Kapiris used the names of legitimate Massachusetts companies for the two Square accounts and created the Amazon account in the name of a company that he controlled, "NetworkingPlus."

Kapiris linked the three vendor accounts to several of his own personal accounts at Bank of America into which he transferred the fraudulent proceeds. Kapiris then used the stolen funds for personal expenses including a $19,250 payment to a home contractor. (Source)

2 Attorneys Of Law Firm Charged With Stealing $320,000 In Legal Fee Fraud Scheme - June 24, 2022

Scott Diamond was an attorney who was a partner in a Philadelphia law firm, and Jesse Cohen was an associate in the same law firm. The firm specialized in complex commercial litigation, representing plaintiffs in personal injury matters, and representing insurance companies in insurance subrogation matters.

For approximately two years from 2018 through 2020, Diamond and Cohen engaged in a scheme to divert the fees from numerous personal injury and subrogation matters from the firm to themselves by secretly resolving the cases without the other firm partners knowing about the resolutions. Diamond and Cohen then caused insurance companies and other payors on those cases to send legal fees to themselves instead of to their employer, the law firm. When that was not possible, Diamond went through the firm's mail and removed checks covering legal fees on the stolen cases made payable to the firm. Diamond then deposited checks from the cases they diverted into bank accounts that he controlled and shared the proceeds with Cohen. Diamond concealed the illegal conduct from his employer by closing the files for those matters and making it appear in the computer records of the firm that there were no settlements or resolutions and that the cases were not viable.

The personal injury and subrogation matters that Diamond and Cohen diverted from the law firm generated approximately $750,000 in initial payments to the defendants, from which they distributed funds to clients and covered other costs in the litigation, maintaining the balance of the fraud proceeds (approximately $320,000) for themselves. (Source)

Former Accounts Payable Clerk Sentenced To Prison For $300,000+ Of Fraud To Pay For His Bills - June 30, 2022

Grant Devillez admitted that from at least February 2016 through July 2018, he engaged in a scheme to defraud Décor Craft, Inc., of nearly $303,000, by transferring funds from the business bank account to his own personal bank accounts to pay for personal bills and to the bank account of another individual.

Devillez also admitted that when given access to the business bank account to make authorized payments to vendors, he often made partial payments or no payments at all, instead transferring the funds for his own use. To cover his criminal conduct, he altered company records to reflect that full payment had been made to the vendors. (Source)

Former Executive Director For Chamber Of Commerce Charged With Misappropriating $300,000 For Personal Use - June 22, 2022

Karen Smith served as the Chamber's Executive Director from 2006 to 2019.

From 2013 to 2019, Smith issued checks from the Chamber's bank accounts to herself and deposited them into her personal accounts. She then spent the money for her own personal use and benefit.

Smith attempted to cover up the fraud by submitting false and misleading financial reports to the Chamber's Board of Directors and false payroll reports to the Chamber's accounting firm, the charges allege. Smith fraudulently misappropriated at least $300,000 in funds belonging to the Chamber. (Source)

Former Employee Sentenced To Prison For Embezzling $295,000+ - June 2, 2022

Between October 2010 and August 2016, Ruby Baroni held an accounting position at a New Jersey guided-tour company. In that capacity, Baroni had authority to cut checks against the company's bank accounts.

During that period, Baroni and Estela Laluf, a manager at the company, devised a scheme to embezzle funds from the company. Laluf would direct Baroni to cut company checks to actual company employees and contractors, which did not reflect any actual work or services done by those individuals. Baroni would then cash these checks, and Laluf and Baroni would then convert the resulting funds to their personal use.

Laluf and Baroni embezzled hundreds of thousands of dollars from the company. (Source)

Former Office Manager Sentenced To Prison For Embezzling $200,000 From Employer For Use In His Side Taxi Business - June 1, 2022

From October 2017 to April 2019, David Jackson worked as the Office Manager. His duties included handling all financial aspects of his employer's business, including collecting, accounting for and paying over trust fund taxes to the IRS on behalf of his employer. Jackson also owned and operated a taxi business in Gillette and Casper.

Between February 2018 and April 2019, Jackson committed wire fraud by embezzling money from his employer, diverting money from the employer's bank account and misusing a company credit card for his own personal expenditures, to include expenses associated with his taxi business. (Source)

SHELL COMPANIES / FAKE INVOICE BILLING SCHEMES

Former Public Schools Employee Sentenced To Prison For Defrauding School District Of $550,000+ - June 8, 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)

Former Operations Manager Pleads Guilty To Embezzling $2.6 Million+ From Shipping Company By Creating Fake Invoices -May 31, 2022

Savino USA provides transportation services to its customers in the United States by subcontracting local deliveries to third-party trucking companies.

In her role at Savino USA, Vika Moa was responsible for selecting and paying these local subcontractors.

Between June 2016, and October 2019, Ms. Moa falsely represented to Savino USA employees that invoices for trucking services were owed, which caused Savino USA to pay more than $2.6 million to a bank account to which she had access.

Moa misrepresented to Savino USA employees that a fictitious business was an actual transportation company. She created fraudulent invoices for trucking services that the fictitious business purportedly provided to Savino USA.

Ms. Moa then directed Savino USA to pay the fictitious business based on these false invoices, knowing full well that the company did not perform any services for Savino USA, as it was not a real business and did not have any operations. (Source)

NETWORK / IT SABOTAGE

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Former Air Cargo Handler Sentenced To Prison For Stealing Gold Bars Headed From Australia To New York - June 27, 2022

Marlon Moody is a former cargo handling company employee at Los Angeles International Airport. He was sentenced to prison for stealing four gold bars that were part of a larger shipment headed from Australia to New York.

A co-defendant, Brian Benson, also pleaded guilty in July 2021 to the same charge.

Both men worked for Alliance Ground International (AGI), a company that provided ground handling services at LAX. On the evening of April 22, 2020, a shipment of gold bars arrived at LAX on Singapore Airlines. A total of 2,000 gold bars, each weighing one kilogram and valued at approximately $56,000, were being shipped at the direction of a Canadian bank. During a stopover at LAX, the gold was offloaded and secured, but an inventory that evening showed one box containing 25 gold bars was missing.

Moody found the missing box of gold bars near the Singapore Airlines cargo warehouse on the morning of April 23, placed the box on a belt loader and drove that vehicle to a nearby location, where he removed four of the bars. Soon after, Benson arrived to pick up Moody in a company van, where they exchanged text messages about the gold bars because other employees were in the van. The two defendants later left the airport and went to a nearby parking lot, where Moody gave Benson one of the four gold bars.

The lost box with the 21 remaining gold bars was discovered by other cargo handlers later on April 23, and authorities began an investigation that ultimately led to Moody and Benson.

Moody gave one gold bar to a relative on May 4 and directed the family member to exchange the gold bar for a vehicle and / or money. Around this time, Moody buried the remaining two gold bars in the backyard of his residence. (Source)

THEFT OF COMPANY PROPERTY

No Incidents To Report

DRUG RELATED INCIDENTS

Prison Corrections Officer & Inmate Charged In Drug Distribution Conspiracy Inside Prison - June 16, 2022

A prison Corrections Officer and an inmate have been charged for their roles in a methamphetamine distribution organization within the Minnesota Correctional Facility (MCF) - Stillwater.

Faith Gratz was a MCF Corrections Officer. Axel Kramer is an inmate who is currently serving a 288 month sentence for second degree murder.

Both conspired with each other to distribute methamphetamine within MCF. As part of the conspiracy, Kramer obtained wholesale quantities of prepackaged methamphetamine from sources of supply outside the prison. After Kramer and another co-conspirator inmate worked with the drug suppliers to arrange meet up times and locations, Gratz would pick up the drug packages. Gratz used her position as a prison guard to smuggle the drugs into the secure facility and then provide the drugs to Kramer while she was on duty guarding him. Gratz did this on approximately six different occasions. Gratz also smuggled into the prison multiple cell phones that she provided to Kramer. Kramer used the cell phones to communicate with people inside and outside the prison and to facilitate his drug distribution network from within the prison.

Gratz and Kramer exchanged hundreds of text messages with each other. The messages included communications about the drug distribution conspiracy as well as discussions about their romantic relationship. Gratz also warned Kramer about upcoming searches of inmates' cells so that Kramer could hide his phone and drugs to avoid detection. (Source)

Former Paramedic Charged With Removing Fentanyl And Replacing With Saline - June 24, 2022

From approximately March 2020 to early October 2020, Candice Mangan, a licensed EMT paramedic in Massachusetts, worked part-time as an EMT for an ambulance service company in Massachusetts.

It is alleged that on or about Sept. 30, 2020, while working in Needham, Mangan tampered with three fentanyl citrate vials by removing fentanyl citrate and replacing it with saline. The liquid remaining in the three vials contained only approximately 4.4%, 6.8%, and 24.2% of the declared concentration of fentanyl citrate. (Source)

Former TSA Officer Pleads Guilty To For Attempting To Smuggle Methamphetamine Through Los Angeles International Airport - June 10, 2022

Michael Williams is a former Transportation Security Administration (TSA) Officer. He pleaded guilty today to a charge for smuggling what he believed was methamphetamine through Los Angeles International Airport (LAX) in exchange for a total of $8,000 in cash.

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

As a TSA employee with unscreened access to LAX, Williams agreed to deliver the methamphetamine in a backpack to the drug source's accomplice in the men's restroom past the airport terminal's security checkpoint.

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

MASS LAYOFFS

No Incidents To Report

WORKPLACE VIOLENCE

McDonald's Employee Charged With First Degree Murder After Killing Co-Worker - June 12, 2022

McDonald's employee Terrence King, a 19 year old, was arrested for a shooting that took place outside a St. Louis McDonald's at around 8:30 p.m.

Kevyn Henderson, 23, was shot in the chest and was not breathing or conscious when officers arrived at the scene and later died.

According to the report, King and Henderson both worked at the McDonald's and got into an argument while inside the fast-food restaurant. The manager of the McDonald's escorted King out of the restaurant.

When Henderson walked out of the McDonald's, King shot and killed him. Police officers took King into custody after locating him with a firearm in his hand near Henderson. (Source)

3 Employees Killed By Co-Worker At Manufacturing Plant - June 10, 2022

3 people were killed and one person was injured at a Maryland manufacturing plant by a co-worker who was also injured following a gunfire exchange with a state trooper.

The shooter, Joe Esquivel went to work at the Columbia Machine factory in Smithsburg and worked his normal shift, authorities said At around 2:30 p.m., he left the building and retrieved a weapon from his car and went back in the plant and opened fire inside a break room. The motive for the shooting is still not clear. (Source)

U.S. Air Force Ordered To Pay More Than $230 Million For 2017 Texas Church Shooting - February 7, 2022

The U.S. Air Force must pay more than $230 million in damages to survivors and victims' families of a 2017 Texas church massacre for failing to flag a conviction that might have kept the gunman from legally buying the weapon used in the shooting, a federal judge ruled.

The judge ruled in that the Air Force was 60% liable for the attack because it failed to submit Kelley's assault conviction during his time in the Air Force to a national database.

An Air Force record of the Kelley court-martial says he pleaded guilty to multiple specifications of assault, including striking his wife, choking her with his hands and kicking her. He also was convicted of striking his stepson on the head and body with a force likely to produce death or grievous bodily harm.

In 2012, several months before his conviction in the domestic violence case, Kelley briefly escaped from a mental health center in New Mexico and got in trouble for bringing guns onto a military base and threatening his superiors there, police reports indicate.

Deputies were called to Kelley's home in June 2013 about the rape case and investigated for 3 months. But it appeared that they stopped investigating after they believed Kelley left Texas and moved to Colorado.

Under Pentagon rules, information about convictions of military personnel in crimes like assault is supposed to be submitted to the FBI's Criminal Justice Investigation Services Division for inclusion in the National Criminal Information Center database. For unspecified reasons, the Air Force did not provide the information about Kelley as required. (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

Former Vice President Of Discovery Tours Pleads Guilty To Embezzling $600,000 Causing Company To Cease Operations & File For Bankruptcy - June 15, 2022

Joseph Cipolletti was employed as Vice President of Discovery Tours, Inc., a business that offered educational trips for students. Cipolletti managed the organization's finances, general ledger entries, accounts payable and accounts receivable. Cipolletti also had signature authority on Discovery Tours' business bank accounts.

From June 2014 to May 2018, Cipolletti devised a scheme to defraud parents and other student trip purchasers by diverting payments intended for these trips to his own personal use on items such as home renovations and vehicles.

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy. Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

Former Credit Union CEO Sentenced To Prison For Involvement In Fraud Scheme That Resulted In $10 Million In Losses, Forcing Credit Union To Close - April 5, 2022

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports. This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union. Godfrey-Smith investigated and discovered that there were millions of dollars of fictitious entries on SFCU's general ledger, and the credit union's books were not balanced. But she failed to disclose this information to the United States Department of the Treasury and signed the false Officer's Statement.

In the Spring of 2017, the credit union failed. An investigation by revealed that SFCU had amassed in excess of $10 million in losses by December 2016. (Source)

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)


Scrn
Scroll Lock
Pause
sabotage
Insert
Home

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 (**3,800+ 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: White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines,) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **900+** 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.

Insider Threat Program Development – Management Training Course / Classroom Based: Sterling, Virginia, August 22 & 23, 2022

In addition to the main instructor, this class will also have 2 additional instructors who are the former ITP Managers for CIA and NSA, and have extensive knowledge of ITP Development - Management in the U.S Government, Department of Defense, Intelligence Community and the private sector.

Complete Details / Registration / Cost: $1,495 With Money Back Guarantee
https://www.eventbrite.com/e/insider-threat-program-development-management-training-course-tickets-381120671187

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