INSIDER THREAT INCIDENTS REPORT
FOR
February 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

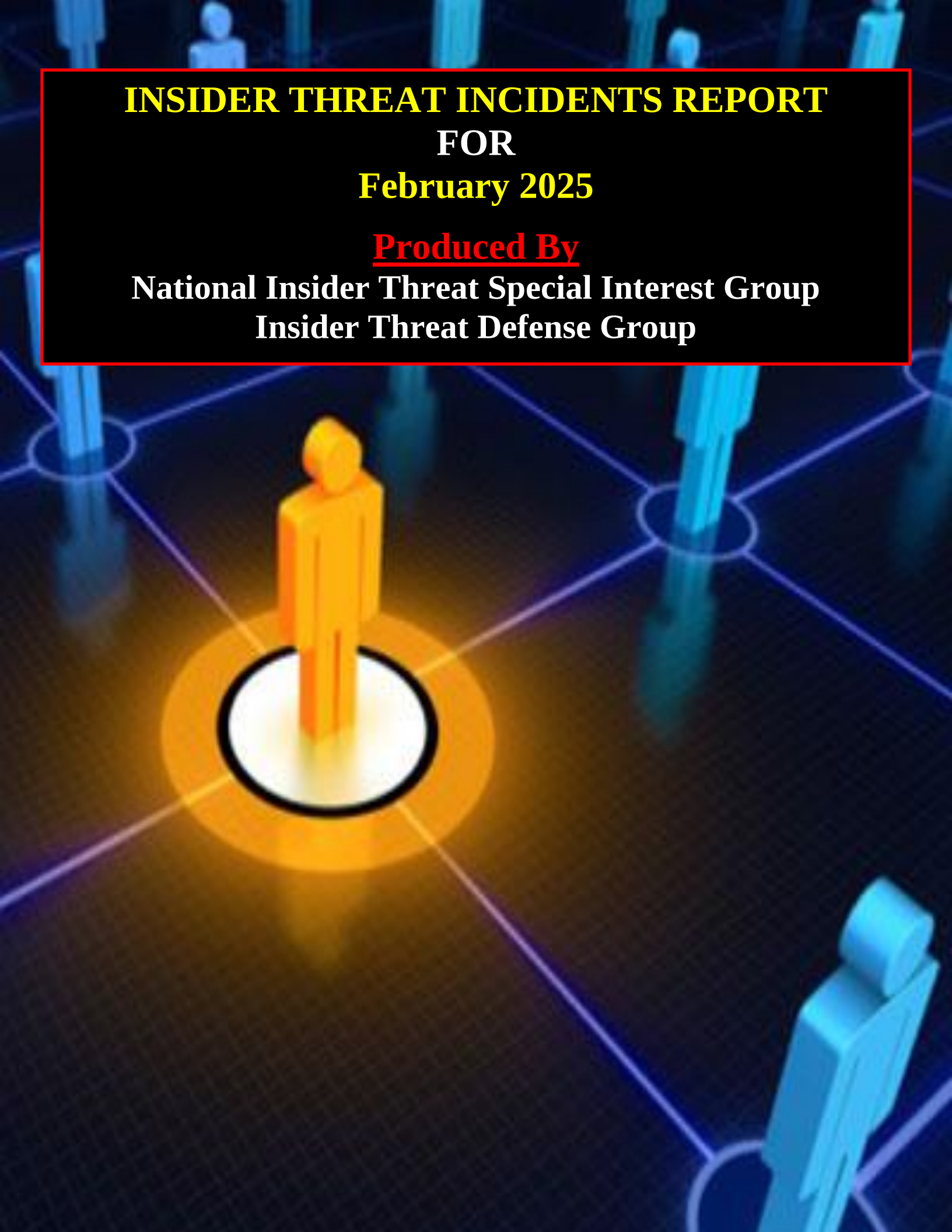

TABLE OF CONTENTS

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 are negligent, malicious or opportunists. 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 15+ years. This research has evaluated and analyzed over **6,000+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

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. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

According to the Association of Certified Fraud Examiners 2024 Report To the Nations, the 1,921 fraud cases analyzed, caused losses of more than **$3.1 BILLION.**

To grasp the magnitude of the Insider Threat problem, one must 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.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the **Actual Malicious Actions** employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live a better lifestyle, etc.

Some organizations invest thousands of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of these monthly reports, you might have a different perspective on Insider Threats.

The Human Operating System (Brain) is very sophisticated and underestimating the motivations and capabilities of a malicious or opportunist employee can have severe impacts for organizations.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report and other shows. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 24** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR FEBRUARY 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT

U.S. Postal Employee And Co-Conspirator Sentenced To Prison For $24 Million Stolen Check Scheme - February 7, 2025

According to court records, from March 2021 to July 2023, Nakedra Shannon was employed by the U.S. Postal Service (USPS) as a mail processing clerk at a distribution center in Charlotte, North Carolina.

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

U.S. Postal Service Supervisor Pleads Guilty To Stealing $300,000+ In Checks, Gold & Collectable Currency From Mail - February 7, 2025

From early last year until December 2024, while on duty with USPS, Joivian Hayes stole mail from the Costa Mesa Post Office in California, including checks that had been mailed, which she then deposited into her own bank accounts by forging the payees listed on the checks.

Hayes stole at least 20 checks totaling approximately $284,000, which she then deposited into her bank accounts at various banks. She also stole and deposited $3,000 in postal money orders that had been mailed. She deposited the stolen checks by using her banks' mobile apps and at ATMs. During some of the ATM deposits, Hayes wore a blue t-shirt bearing a USPS logo.

During a search of Hayes' residence, law enforcement found multiple gold coins and bills of U.S. currency that had been sent by registered mail. Hayes had stolen these items from the Costa Mesa Post Office. Among those items included a $1 bill dating from 1917 with a sticky note listing a value of $675, a $100 bill dating from 1914 valued at $1,500, and a $10 Confederate States of America bill.

Federal agents also found various gold pieces, including a $5 gold piece with sticky note listing a value of $1,600. Federal agents also found inside Hayes' bedroom a pink wallet with a U.S. Treasury check payable to a victim in the amount of $2,599, addressed to a location in Costa Mesa, which defendant had also stolen from the mail at the Costa Mesa Post Office.

The intended loss from Hayes' theft of mail is approximately $304,000 to $324,288, which is comprised of approximately $284,000 in stolen checks that Hayes deposited into her various bank accounts and approximately $20,000 to $40,000 in other items she had stolen from the mail, including gold coins and currency. (Source)

U.S. Postal Service Employee Sentenced To Prison For Stealing $95,000 In Cash, Gift Cards & Checks From Mail - February 27, 2025

This conduct occurred multiple times per week. During December 2023, when Willie Estrella participated in the conspiracy, $95,000 in cash, gift cards, and checks were illegally removed from the U.S. mail stream and stolen by Estrella and others.

Estrella and others sorted through the mail at the Providence distribution facility and placed aside brightly colored envelopes of interest. They concealed the stolen mail in their backpacks that they carried from the postal facility. Estrella and co-conspirators met at a pre-determined location after work to open the stolen mail and remove cash, gift cards, and checks. They divided the proceeds among themselves. (Source)

U.S. Postal Service Employee Admits Stealing 100+ Mail Packages - February 13, 2025

Zachary Simpson admitted to theft, after he was accused of stealing mail when he tried to sell $850 worth of sports cards to a Billings sports memorabilia business that had attempted to ship the cards to a different customer.

Between March 27, 2023 and April 3, 2024, Simpson was employed by the U.S. Postal Service and sorted packages at the mail facility in Billings. Simpson had access to and was entrusted with mail during his shifts at the sorting facility.

While employed with the Postal Service, Simpson stole packages from the sorting facility and took them home. On March 12, 2024, the U.S. Postal Service Office of Inspector General was contacted regarding Simpson. A sports memorabilia business in Billings notified law enforcement that Simpson came into the store to sell $850 of sports cards. The company realized that it had recently attempted to ship those same cards to a different customer through the mail. An investigation determined that the packages containing these cards had transited the postal sorting facility in Billings on a date Simpson was working. Law enforcement conducted a trash pull at Simpson's residence and found dozens of empty packages in his trash that were addressed to other people at different locations. Investigators executed a search warrant at Simpson's residence and seized more than 100 additional empty packages that were not addressed to Simpson. Agents also recovered more than 10,000 sports trading cards and other memorabilia. The Postal Service contacted a number of the victims whose packages were found in Simpson's possession. Many reported that their packages contained sports trading cards that never reached the intended destination. (Source)

Employees With The IRS And U.S. Postal Service Are Among 3 Individuals Charged For Stealing And Cashing A $72,000 U.S. Treasury Check - February 10, 2025

Sierra McCall, 31, and Jalen Koonce, 31, and Julian King, 31, where charged.

McCall is employed by the IRS as a customer contact representative. Koonce is employed by the U.S. Postal Service at the sorting facility where government checks are processed. King is the father of McCall's child.

McCall, Koonce, and King together aided and abetted each other to steal and cash a $72,236 U.S. Treasury check on Aug. 9, 2023. (Source)

Social Security Administration Claims Specialist Sentenced To Prison For Creating Fake Children's Profiles To Steal $75,000+ - February 26, 2025

Lee Nichols intentionally misused the identities of vulnerable individuals, including a man who originally applied for benefits after being diagnosed with a terminal illness. Nichols waited until this man died before creating the fraudulent application and then withdrew the benefits using a debit card at drive-thru ATMs where he concealed his identity using masks and other coverings. The court also heard how Nichols' flight from justice wasted government and court resources and how, by taking his luxury pickup truck to Mexico, Nichols prevented the truck from being sold for restitution.

Nichols originally admitted to creating fictitious profiles for two children that did not exist. He linked the profiles to a recently deceased man and disabled woman living in Mexico in an attempt to create a survivor benefits application.

Nichols also ensured that the debit cards for the children's benefits were sent to the address of someone with whom he was associated. He would then use the debit cards to make regular withdrawals at ATMs. When making those withdrawals, he attempted to disguise himself by using hats pulled down over his face, sunglasses, balaclavas and other clothing to conceal his appearance.

In addition, the IRS issued economic stimulus payments of $1,400 to each fictitious child pursuant to the Coronavirus Aid, Relief and Economic Security Act.

As part of his plea, Nichols took responsibility for over $75,000 in loss to the federal government. He also agreed to pay $82,516 in restitution to the SSA and $2,800 in restitution to the IRS. (Source)

Former Illinois Speaker Of The House Michael Madigan Convicted On Federal Conspiracy And Bribery Charges - February 12, 2025

Former Speaker of the Illinois House of Representatives Michael Madigan was convicted on conspiracy and bribery charges for using his official position to corruptly solicit and receive personal financial rewards for himself and his associates.

Evidence at trial revealed that Madigan, who served as House Speaker and occupied a number of other political roles, conspired with others to cause the utility company Commonwealth Edison to make monetary payments to Madigan's associates as a reward for their loyalty to Madigan, in return for performing little or no legitimate work for the business. The true nature of the payments was to influence and reward Madigan in connection with specific legislation ComEd sought in the Illinois General Assembly.

Madigan was also convicted of scheming to accept legal work unlawfully steered to his private law firm and his son by an Alderman of the Chicago City Council, in exchange for Madigan's assistance in inducing the Governor of Illinois to appoint the Alderman to a compensated State Board position. (Source)

Employee For IT Asset Disposition Company Pleads Guilty To Theft & Sale Of Hundreds Of Government Phones & Computers Slated For Destruction - February 4, 2025

Between February 2019 and September 2023, Nikhil Parekh was a driver for an international IT asset disposition company, which operated out of Maryland and, later, Virginia. Several government agencies as well as private companies in the region contracted with the company to take older, obsolete IT assets and completely dismantle and recycle them in a responsible manner. These services including wiping and sanitizing digital storage devices in accordance with nationally promulgated standards.

From 2022 to 2023, Parekh and his unindicted co-conspirators served as drivers for the company and were generally responsible for receiving the IT assets from the victim agencies and companies and either securely shredding them on site or delivering them to secure shredding facilities owned by the company. Instead, however, as Parekh admitted, he and others would surreptitiously remove the IT assets after receiving them and transport them to electronics re-sellers in the area for their own accounts. After pocketing the profits, Parekh and others would then cause the company to issue certificates to the victim agencies and companies certifying that the IT assets had been wiped and destroyed. Parekh admitted that as part of this conspiracy he and others took hundreds of assets with a value of at least $10,000.

Investigating agents of the U.S. Capitol Police and USAID, noting that some of the resold devices still had their government asset tags on them, tracked down evidence of the transfer / sale of devices furnished by the victim agencies and companies from resellers in the area and beyond. (Source)

Former Social Security Administration Employee Pleads Guilty To Attempting To Induce A Social Security Beneficiary For Prostitution - February 28, 2025

In March 2024, Dae Kim handled an in-person visit at the Gardner SSA field office from an individual seeking Social Security benefits after losing her job. After redirecting the individual to another SSA field office near her residence in another state, Kim called the individual, using the phone number he obtained from SSA's computer system. Kim indicated that he understood she was in a difficult situation and stated that maybe they could "work something out" that would benefit them both.

During a call monitored by law enforcement later that month, Kim again stated to the individual that they could "help each other out" and proposed giving the individual money in exchange for sex.

In several subsequent text messages, Kim suggested that the individual travel to Massachusetts to meet him, offering to pay $100 to have sex in a car at a hotel parking lot. When Kim traveled to the hotel parking lot to meet the individual in October 2024, he was confronted by law enforcement. (Source)

IRS Contractor Sentenced To Prison For Leaking 400,000+ Tax Returns - February 26, 2025

The IRS told House Republicans this month that a former contractor leaked the private data of more than 400,000 taxpayers, nearly six times higher than originally thought.

Doug O'Donnell, the acting IRS commissioner, told House Judiciary Chair Jim Jordan (R-Ohio) that the agency had informed 405,427 taxpayers that the contractor, Charles Littlejohn, had leaked information from their tax returns or other agency forms.

About nine in 10 of those contacted were businesses, O'Donnell told Jordan. But those returns could also include individual information.

Littlejohn was sentenced to five years in prison last year for the disclosures, which included returns for both President Donald Trump and Elon Musk. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Navy Sailor Pleads Guilty To Plotting To Attack Naval Station On Behalf Of Iran - February 27, 2025

A former Navy sailor (Xuanyu Pang) has pleaded guilty in federal court to plotting to attack Naval Station Great Lakes in North Chicago, Ill., purportedly on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC).

Pang communicated in the summer of 2021 with an individual in Colombia about potentially assisting with a plan involving Iranian actors to conduct an attack against the United States to avenge the death of Qasem Soleimani, a general of the IRGC Quds Force who was killed by the U.S. military in 2020. The Quds Force is a branch of the IRGC that conducts unconventional warfare and intelligence activities outside of Iran. (Source)

U.S. Army Soldier Sentenced To Prison for Attempted Murder Of Another Solider - February 27, 2025

Allen James, 46, entered the barracks room of another soldier while she was sleeping and attempted to rape her at knifepoint. The victim resisted and was repeatedly stabbed. After James left the room, she escaped and reported the incident before she was taken to the hospital for emergency surgery for stab wounds.

Medical records revealed that one of the victim's neck wounds was within millimeters of her jugular vein and penetrated from the front to the back, nearly reaching her spine. As a result of the stabbing, the victim sustained permanent nerve damage.

When a DNA profile did not produce a match and a suspect was not identified, the case went cold until 2019. Through new DNA analysis by the United States Army Criminal Investigation Laboratory (USACIL), the Department of the Army Criminal Investigation Division (CID) was able to identify James as the perpetrator and locate him while he was stationed at Fort Belvoir, Virginia in March 2021. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Fire Department Administrator Sentenced To Prison For Causing 26 Arson Fires In National Forest / Cost $638,000+ - February 10, 2025

A former fire department administrator and police officer was sentenced to 18 months in prison for starting dozens of arson fires in Wayne National Forest in Ohio.

James Bartels, 52, started 26 fires in the national forest in 2022, creating a substantial risk of death or significant injury to the public, as well as to firefighters from federal, state and local governments who were summoned to extinguish the fires.

In total, more than 100 firefighters from several states responded to the fires. Approximately 1,300 acres of federal and state land were burned, and the U.S. Forest Service incurred more than $638,000 in resulting expenditures.

At the time, Bartels was an administrator at the Greenfield Township Volunteer Fire Department. He also served as a police officer at various law enforcement agencies in Ohio and a 911 dispatcher for Gallia County.

The Ohio Department of Natural Resources law enforcement officers observed a truck registered to Bartels near Wayne National Forest on Oct. 29, 2022. Within an hour, a fire was reported in the forest near where Bartels had been.

In the days after Bartels's Nov. 8, 2022, resignation from working as a 911 dispatcher for Gallia County, at least 17 fires were lit.

Bartels was seen at two separate locations in the vicinity of multiple fire starts within minutes of their ignition. His truck's infotainment system data also placed him at the locations of the fires.

Bartels admitted to starting the fires with a lighter to "give the boys something to do" and to distract himself from his depression.

The defendant was arrested in December 2022 and pleaded guilty in September 2023. As part of his sentence, Bartels was ordered to pay $638,000 in restitution and register through the Ohio Arson Registry. (Source)

DHS Deportation Officer Pleads Guilty To $700,000 Drug Money Laundering - February 27, 2025

Over a two-month period in 2023, Christopher Toral agreed to transport $700,000 in drug proceeds under the protective cover of his position as a federal law enforcement officer.

As part of an undercover operation, Toral agreed to transport a black bag containing $200,000 in cash from Dallas to Houston in February 2023. He believed this money was revenue from the sale of illegal narcotics. Later that same month, Toral repeated the trip, delivering an additional $200,000.

In March 2023, Toral agreed to transport $300,000 from Newark, New Jersey, to Houston on a commercial flight. The money was represented to be the proceeds of drug trafficking. While carrying the illicit gains, Toral bypassed airport security and Transportation Security Administration checkpoints by exploiting his law enforcement position. Toral did all this in exchange for cash payments. (Source)

U.S. Customs & Border Protection Officer Convicted Of Smuggling Cocaine From U.S. Virgin Islands To Atlanta - February 26, 2025

On January 10, 2020, Ivan Van Beverhoudt, a former U.S. Customs and Border Protection officer, boarded a commercial flight from St. Thomas, U.S. Virgin Islands to Atlanta with 16 bricks of cocaine in two carry-on bags.

To avoid TSA screening in St. Thomas, Van Beverhoudt traveled in his official capacity with his loaded CBP-issued firearm. Upon arriving at the Atlanta Hartsfield-Jackson International Airport, en route to his final destination of Baltimore, Maryland, a trained narcotics K-9 officer in the jetway alerted to Van Beverhoudt's luggage, resulting in the discovery of the cocaine. (Source)

County Sheriff Sentenced To Prison for Soliciting, Accepting $9,500 Bribes And Providing Ammunition To A Convicted Felon - February 11, 2025

Marshand Crisler, 55, was appointed as the Sheriff of Hinds County in Mississippi on August 2021.

The evidence at trial showed that shortly after becoming Sheriff, Crisler solicited and accepted $9,500 in cash bribes from a convicted felon over three months, from September through November of 2021. In exchange for that money, Crisler agreed to provide favors through his position as Hinds County Sheriff.

These favors included sharing information concerning future criminal investigations involving the bribe payor, moving a jailed family member to a better place within the Hinds County Jail, and hiring the bribe payor to work at the Hinds County Sheriff's Office. Crisler also gave ammunition to the bribe payor, knowing that the person was a convicted felon. (Source)

2 Police Department Employees (Chief, Captain) Plead Guilty To $149,000+ Overtime Fraud / Some Fund Were Federal Grants - February 13, 2025

Michael Redmon and Darin Cathell spent years claiming to work overtime shifts that they did not work. Redmon, the former Chief of the Department, falsely claimed at least 174 shifts, totaling at least 760 hours and at least $81,890. Cathell, the former second-in-command of the Department, falsely claimed at least 185 shifts, totaling at least 800 hours and at least $67,970. Some of the funds Redmon and Cathell received were federal grant funds. (Source)

Baltimore Sheriff Directed His Staff To Use Code On Timesheets To Boost Their Wages That Was Not Authorized Resulting In $2.2 Million Of Overpayment To Officers - February 12, 2025

Baltimore Sheriff Sam Cogen directed his staff to use a code on electronic timesheets to boost their wages, triggering an improper calculation that cost the city more than $2.2 million, the city's inspector general has found.

The "incorrectly issued" payments, which have not been returned to the city, were made after Cogen instructed sheriff's office employees to enter hours in the city's online timekeeping system as "city detail overtime," according to a report from Inspector General Isabel Cumming that was released. The coding was intended to pay deputies an additional $31,200 annually, Cumming said.

However, the pay code was mis-configured in the city's timekeeping system, a detail that Cogen told the inspector general he was unaware of, the report said. As a result, 94 deputies who followed Cogen's instructions were paid triple the amount they were due for a standard workday.

The inspector general found that the sheriff's office "did not exercise due diligence" in monitoring the order's impact on the department's budget. Cogen did not notify city finance officials or human resources and financial staff within his own office, the report found.

The de facto pay increases for the sheriff's staff were enacted after Cogen failed to get approval for pay increases following standard procedure. After his election in 2022, Cogen, a Democrat, sought Mayor Brandon Scott's blessing to use about $2 million in available funds within the sheriff's budget to pay for increases.

Cogen implored the mayor to sign off, according to an October 2023 letter detailed in the report. Scott did not respond until January, writing that the city would not address requests for salary increases until the next round of labor negotiations. Scott told Cogen that he could not use the available funds for increases and noted that the city already agreed to cost-of-living increases for deputies through 2025.

By then Cogen had already sent a memo to staff in November 2023 directing them to file hours using the "city detail overtime" pay code. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

2 Arizona Department Of Economic Security Employees Convicted Of Embezzling $3 Million+ & Receiving Bribes To Approve Unemployment Insurance Claims - February 11, 2025

Both Jacqueline Espino and Brandilyn Lorenzen were employed by the Arizona Department of Economic Security (DES) as adjudicators who evaluated claims for both unemployment insurance (UI) and Pandemic Unemployment Assistance (PUA).

Between 2020 and 2022, when DES was facing a higher volume of UI and PUA claims as a result of the COVID-19 pandemic, Espino and Lorenzen each accepted bribes to approve UI and PUA claims for individuals

who were not qualified to receive such assistance. In addition, both Espino and Lorenzen admitted that they embezzled large sums money from DES for their own benefit and for the others.

Espino admitted in her plea agreement that she received bribes related to 9 UI/PUA claims, which caused DES to pay $140,298 in claims that were not properly adjudicated by DES. During the same period of time, Espino also embezzled $600,672 in DES funds for her own benefit and others.

Lorenzen admitted in her plea agreement that she received bribes related to 24 UI/PUA claims, which caused DES to pay $532,964 in claims that were not properly adjudicated by DES. During the same period of time, Lorenzen also embezzled $2,461,520 in DES funds for her own benefit and others. At her sentencing, Lorenzen was ordered to pay $2,994,484 in restitution to DES. (Source)

Former County Health Department Official Pleads Guilty To Embezzling $260,000 / Used Funds To Pay Credit Card - February 20, 2025

Hugo Huacuz is a former employee of the Taney County Health Department in Missouri.

Huacuz embezzled approximately $260,000 from the agency between March 23, 2022, to Nov. 14, 2023.

Huacuz caused the health department to write checks to Argon Investments, LLC, a company organized by Huacuz and his wife. Huacuz forged the signatures of health department members, using their identities without their permission. Huacuz caused the health department to issue 15 checks totaling approximately $259,000, which were deposited into the bank account of Argon Investments.

Huacuz used the stolen funds for personal expenses charged to his personal credit card, including automobile insurance, maintenance, repair and parts; restaurants; home construction items; gasoline; airline tickets and travel, including to Chicago, Illinois, New York State, San Diego, California, College Station, Texas, Nashville, Tennessee, Las Vegas, Nevada, and Portland, Oregon; utilities; dry cleaning; clothing; dental and medical care; and payments to the Missouri Secretary of State's office for Argon's LLC fees.

Health board members were not aware of the existence of Argon Investments or that any checks had been issued to Argon Investments. In order to conceal his scheme from the board, Huacuz caused these checks to be coded as payments to Sanofi Pasteur, Inc., a multinational pharmaceutical company. Huacuz falsely reported to the health department's board that some of the checks written to Argon Investments were for items purchased from Sanofi, and created false invoices from Sanofi purportedly for the purchase of pharmaceutical and medical items, including COVID-19 testing kits.

In November 2023, the director of the Taney County Health Department received information concerning Huacuz's job performance. The information stated that Huacuz was frequently absent from his job and that he had other businesses he was operating independent from his job at the health department. After reviewing the information, the director met with Huacuz on Nov. 13, 2023, and placed him on administrative leave. Huacuz went to the bank immediately afterward and withdrew more than $24,000 from the Argon bank account, leaving a balance of $100 in the account. (Source)

New York City Housing Authority Superintendent Sentenced To Prison For Accepting $50,000+ In Bribes For Contract Work / 70 Others Involved - February 26, 2025

Joy Harrios, a former superintendent for the New York City Housing Authority (NYCHA), was sentenced to prison for soliciting and accepting over $50,000 in bribes from contractors in exchange for awarding those contractors at least approximately $500,000 in contract work.

Of the 70 individual NYCHA employees charged with bribery and extortion offenses who were arrested in February 2024, 61 have pled guilty, and three have been convicted after trial. Harris is the first of the three NYCHA employees convicted after trial to be sentenced. (Source)

Executive Director For County Recreation Authority Sentenced To Prison For Embezzling $16,000+ / Use Funds To Purchase Property - February 11, 2025

Melissa Rose is the former Executive Director of the Southwest Regional Recreation Authority (SRRA).

Rose was sentenced yesterday to time served plus three years of supervised release and was ordered to pay $16,614 in restitution for bank fraud and embezzlement associated with her scheme to steal money intended for SRRA's Spearhead Trail System.

The SRRA was established in 2008 to oversee the development and management of the Spearhead Trail System. Spearhead Trails consists of three outdoor recreation tourism destinations within its complex. The SRRA receives approximately $1.1 million of general funds per year to operate, including federal funds.

Rose was hired on July 23, 2019, as the Sales and Finance Manager for SRRA. The SRRA Board of Directors promoted Rose to Executive Director in October 2021. As Executive Director, Rose was responsible for the day-to-day operations of the SRRA and the Spearhead Trail System. She resigned from her position on February 3, 2023, following an investigation concerning embezzlement of SRRA funds.

On January 23, 2023, the SRRA learned that Rose had used SRRA funds for her personal use. Specifically, Rose wrote $16,614 in checks drawn on the SRRA's bank account that were purportedly signed by another SRRA board member. The checks were drawn on the SRRA First Bank and Trust Company account and were for the purchase of a residential property priced at $69,5000 with a $15,000 down payment.

The property was for Rose's personal use. In an attempt to hide her fraud, Rose logged her payments for the residential property into the SRRA's QuickBooks account management system as purchases for "Tools" with "Land Lease for 5 Years on Mountainview Trail for Conex & SXS Storage" written in the description. She also prepared a fraudulent purchase order and a fraudulent lease for the property, again forging a signature of another SRRA employee. Rose also fraudulently utilized her Notary Public credentials to notarize the signatures she forged. (Source)

New York City Fraud Investigator Sentenced to Prison For Stealing Homeless Victims' Identities To Apply For Unemployment Benefits - February 5, 2025

Olabanji Otufale is a former New York City Department of Homeless Services Fraud Investigator.

At the time of the scheme, Otufale was a fraud investigator with the New York City Department of Homeless Services (The Department).

In that role, Otufale was responsible for ensuring individuals who applied for homeless services such as housing in homeless shelters, were qualified to receive services from the department.

In the fall of 2020, Olabanji Otufale conspired with others to steal the personal identifying information of more than ten homeless individuals and use that stolen information to fraudulently apply for unemployment insurance benefits in the names of those homeless individuals without their knowledge or consent.

Otufale, however, used his access to a database maintained by the Department to commit fraud himself, stealing the personal identifying information, names, social security numbers, dates of birth of vulnerable victims who

had given that personal information to the department when they applied for services. Otufale then texted this victim information to a co-conspirator, Marc Lazarre, who applied online for unemployment benefits in the names of the homeless victims. Otufale and Lazarre conspired to split the fraudulent benefits they received. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School District Employee Sentenced To Prison For Embezzling $135,000+ - February 27, 2025

Linda Johnson committed the embezzlement while employed in an administrative support role in the superintendent's office between 2016 and 2022.

Johnson was responsible for depositing cash and checks into the district's activities account intended to support student athletics, clubs and extracurriculars. She stole donations and funds raised to support yearbook, cheer, dance, vending machines, trivia nights, science clubs, ROTC and more.

To conceal her crime, Johnson drafted bank deposit slips reflecting the correct amount of cash and checks received, but later she prepared a second set of fraudulent deposit slips that only accounted for the checks, while she kept the cash.

Johnson committed 165 fraudulent transactions, and the loss to the school district was $135,566.80. (Source)

University Employee Charged With Stealing & Selling Stolen Apple Products - February 13, 2025

Tung Pham worked as a facilities and purchasing coordinator for the library of a public university in San Jose, CA. In that position, Pham was entrusted with a university procurement card to purchase necessary items for the library.

Pham, however, used the procurement card to purchase, among other things, Apple MacBooks and Apple iPads that he stole and sold to others for personal gain, including a co-conspirator who lived in Folsom. The individual in Folsom resold and shipped the stolen Apple products to buyers outside the State of California. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Labor Union Financial Secretary Pleads Guilty To Embezzling $14,000+ Of Union Assets - February 6, 2025

From approximately April 2013 through April 2021, Vincent Wolf served as the financial secretary for the United Steelworkers Local Union 623 in Freedom, Pennsylvania. As financial secretary, Wolf was responsible for maintaining all financial records, preparing annual reports, and issuing payments on behalf of Local 623 related to union officers' salaries and expenses.

An audit of the union's finances following Wolf's re-election loss revealed that Wolf omitted from those records disbursements that he made to himself in the form of writing union checks to himself, ATM withdrawals, and using the union debit card to buy lunch and alcohol. The audit determined that Wolf embezzled a total of $14,695. (Source)

BANKING / FINANCIAL INSTITUTIONS

Bank Of America Employee Pleads Guilty To Role In $25 Million International Money Laundering Conspiracy - February 27, 2025

In May 2023, Rongjian Li was among 12 individuals from Massachusetts, Rhode Island, New York and California charged in a superseding indictment for their alleged involvement in a sophisticated international money laundering and drug trafficking organization led by Jin Hua Zhang.

The investigation revealed that, for a fee, Zhang laundered bulk cash for drug dealers and laundered profits from other illegal businesses. In less than a year, Zhang and his organization laundered at least $25 million worth of drug proceeds and funds from other illegal businesses through undercover agents. Funds were eventually traced to, and seized from, accounts in Hong Kong and elsewhere in China, India, Cambodia and Brazil, among other locations.

The investigation identified Li as a member of the money laundering conspiracy who, from 2021 through 2022, used his position as a Bank of America employee to knowingly open several accounts through which the organization laundered illicit funds. Li was also aware that some of the accounts were opened using fraudulent passports. As part of his involvement, when the bank's financial auditing systems flagged or froze accounts for suspicious activity, Li helped Zhang circumvent the bank's anti-money laundering protocols and move illicit funds elsewhere. In addition, Li was observed sitting next to Zhang at a dinner in New York, where Zhang discussed the different fee percentages he charged various criminal groups for drug trafficking and scams. (Source)

Bank Teller For JP Morgam Chase Charged For Role In Cashing $850,000 Of Stolen U.S. Treasury Checks - February 13, 2025

From around May 2022 through March 2023, Franchesca Calagui and Dondre Gray conspired to obtain stolen U.S. Treasury checks, recruit others to fraudulently endorse or sign the stolen U.S. Treasury checks, and give the checks to Calagui to cash for the defendants' personal benefit. At the time, Calagui was a part-time associate banker at JP Morgan Chase Bank.

Credit Union Employee Sentenced To Prison For Embezzling $389,000 By Swapping Real Money For Fake Currency - February 26, 2025

From about July 2023 to June 2024, Edward Nurse embezzled from his employer, Park Side Credit Union in Missoula. In June 2024, an employee discovered $340,000 in cash in the credit union's vault had been replaced with fake funds from a company that provides fake currency as props for movies and entertainment productions. Nurse used his position as "team lead" for the vault to swap the credit union's cash with fake money he purchased specifically for this purpose. Nurse hid his conduct from security cameras, auditors and his colleagues by putting real money at the front and back of bundles of fake money. Nurse made multiple purchases of fake money and stole the real cash from his work at different times over a seven-month period.

After the credit union discovered the thefts, Nurse claimed to an FBI special agent that he did not usually carry much cash and, aside from a vacation to Las Vegas, Nevada, he had not made any recent large purchases or cash deposits. However, records show that Nurse made at least nine cash deposits of over $10,000 each in 2024 into his personal account. The investigation also determined that during the first six months of 2024, Nurse had purchased $410,000 in fake currency from a prop money company. The credit union was later informed that approximately $50,000 in fake money had been received by the Federal Reserve in July 2024. Those funds were returned and determined to be fake bills from the prop money company. (Source)

Federal Credit Union Manager Sentenced To Prison For Embezzling $200,000+ From Elderly Clients Forcing Credit Union To Shutdown - February 6, 2025
Gloria Hall was employed at Prairie View Federal Credit Union (PVFCU) in Texas, from 2017 through 2019.

While acting as manager, she purposefully maintained an antiquated business practice which would not allow customers to access their accounts online. Hall admitted she was able to and did access at least two elderly customer accounts and misappropriated $211,563.12 of their funds for her own personal gain.

PVFCU was one of the oldest continually operational federal credit unions a historically black college or university had established in the United States. It did not survive Hall's embezzlement. PVFCU existed for approximately 85 years prior to its failure and merger with the Cy-Fair Federal Credit Union in early 2022. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

2 Chinese Companies Conspired With Former Employees Of Philips Medical Systems To Steal Trade Secrets - February 13, 2025
Philips owned and operated a facility in Aurora, Ill., that engaged in the research, development, and manufacture of X-ray tubes used in computed tomography (CT) medical imaging machines.

China-based KUNSHAN GUOLI ELECTRONIC TECHNOLOGY CO. LTD. and a Kunshan GuoLi vice president, XIAOQIN DU, 63, of Suzhou, China, helped form a rival X-ray tube development company and headquartered it in Aurora.

In 2017, Kunshan GuoLi and Du recruited and hired for the new company three engineers from Philips' Aurora facility, CHIH-YEE JEN, FINCE TENDIAN, and VLADIMIR NEVTONENKO.

The indictment alleges that before the end of his employment at Philips, Jen copied, without authorization, Philips' X-ray trade secret information from internal Philips databases. Jen stole the proprietary information on behalf of Kunshan GuoLi and Du, the indictment states.

Jen used the stolen information in connection with his work developing X-ray tubes at the rival X-ray tube development company for Kunshan GuoLi and a related Chinese company, KUNSHAN YIYUAN MEDICAL TECHNOLOGY CO. LTD., the indictment states. Jen then shared the information with Tendian, who used it in her work for the new company, the indictment states. Nevtonenko also allegedly possessed and used the stolen information in his work there. (Source)

Former Google Engineer Charged With Stealing AI Trade Secrets For China Startup Company / Uploaded 1000+ Files To Personal Account - February 6, 2025
A Chinese national is facing multiple charges of economic espionage and theft of trade secrets after he was accused of stealing artificial intelligence technology from Google.

Leon Ding, 38, was charged with using his position as an engineer at Google to steal code and configuration details for parent company Alphabet's AI projects and then using the pilfered data as the basis for a startup company in China.

If sent to the U.S., he would face seven counts each of economic espionage and theft of trade secrets. Ding could face a maximum of 15 years in prison, if convicted. This, of course, would be contingent on Ding either returning to the U.S. or being arrested and extradited.

The case goes back to May 2022, when Ding was working for Google as a software engineer. Ding is alleged to have copied and uploaded more than 1,000 files to a personal account between May 2022 and May 2023.

Authorities believe that the files, all related to AI software and the underlying hardware configurations used to support AI installations, were taken with the intention forming the basis of a new company in China.

U.S. authorities say that once armed with the confidential code and configuration details from Google, Ding absconded to mainland China, where he got backing from the Chinese Communist Party to start a company with himself listed as founder and CEO.

"Ding circulated a PowerPoint presentation to employees of his technology company citing PRC national policies encouraging the development of the domestic AI industry," the Justice Department said.

"He also created a PowerPoint presentation containing an application to a PRC talent program based in Shanghai." (Source)

CHINESE / NORTH KOREA FOREIGN GOVERNMENT ESPIONAGE / THEFT OF TRADE SECRETS INVOLVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES

National Sales Director For Medical Diagnostic Company Charged In Kickback Scheme That Resulted In $70 Million+ Of Medicare Fraud - February 25, 2025

From at least June 2013 through at least September 2020, David Fuhrmann conspired with others, including two managers for a mobile medical diagnostics company that performed transcranial doppler (TCD) scans, to enter into kickback agreements with various doctors.

Fuhrmann and his co-conspirators agreed to offer and pay doctors kickbacks based on the number of TCD ultrasounds the doctors ordered. Some doctors were paid in cash and others by check. Fuhrmann and his co-conspirators allegedly created rental and administrative service agreements. On paper, these agreements made it appear as if doctors were compensated for the TCD company's use of space and administrative resources based on fair market value and not based on the volume or value of referrals. These agreements were allegedly shams that hid the true nature of the arrangement of paying per test.

The scheme resulted in fraudulent bills of approximately $70.6 million to Medicare. (Source)

Amtrak Employee Admits Participating In $11 Million Health Care Fraud / Kickback Scheme - February 11, 2025

From January 2019 through June 2022, Anthony Saloka and his co-conspirators engaged in a scheme to obtain cash kickbacks from health care providers in return for allowing the providers to use their personal and health insurance information to submit fraudulent claims for services that were either never provided or which were medically unnecessary.

Saloka received thousands of dollars in cash kickbacks from health care providers in return for his participation in the scheme, including from Punson Figueroa, an acupuncturist, and Michael DeNicola, a podiatrist.

Figueroa previously pleaded guilty to conspiracy to commit health care fraud and was sentenced on September 24, 2024 to 34 months in prison.

DeNicola previously pleaded guilty on June 29, 2022 to conspiracy to commit health care fraud, among other offenses. His sentencing remains pending.

In total, the Amtrak health care plan paid over $11 million as a result of fraudulent claims associated with providers connected to the health care fraud scheme. (Source)

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING / INSIDER TRADING / STOCK TRADING & SECURITIES FRAUD

Company Project Manager Sentenced To Prison For Diverting $2.8 Million From Money Paid By Government Contract Awards To Himself - February 24, 2024

Daniel Lee worked as project manager for Agile Infrastructure Service, LLC, in South Carolina.

As project manager, Lee represented Agile in the bidding process to obtain government contracts.

Once Agile was awarded a project, Lee diverted money paid by the government for work on the project to corporations under his control. Lee was then used the funds for his own benefit. The illegally obtained funds totaled at least $2.8 million. (Source)

Vice President / Controller For Publicly Traded Company Pleads Guilty To $1.6 Million+ Insider Trading Scheme - February 4, 2025

Stephen George, 54, was a member of the Finance Department at Company A from November 2017 until April 7, 2023, where he held roles including vice president and controller. Company A is a consumer-packaged goods company headquartered in Boca Raton, Florida, that is the maker of a fitness drink and whose securities are publicly traded on the NASDAQ Stock Market. In his role at Company A, George received material non-public information (MNPI) regarding Company A's profit and revenue performance.

George's last day of employment at Company A was April 7, 2023. On that day, George used a Company A computer to generate out of Company A's enterprise resource planning system a consolidated income statement showing Company A's financial performance for the first quarter of 2023, which George knew contained MNPI.

The income statement showed that Company A's first quarter of 2023 had greatly exceeded expectations. Shortly after generating the income statement, George emailed it to himself using two personal email accounts.

Beginning on April 10, 2023, the first trading day after his last day of employment with Company A, and continuing through May 8, 2023, George purchased Company A securities on the basis of MNPI — specifically, 20,000 shares of Company A common stock and 300 call option contracts.

On May 9, 2023, after the market close, Company A publicly reported better-than-expected earnings and sales for the first quarter of 2023, including an all-time quarterly record in revenue. After the public announcement, Company A's stock price increased significantly. During the next trading day, May 10, 2023, George sold all 20,000 shares of common stock and 300 call option contracts, resulting in over $1.6 million in personal profits. (Source)

Contracting Company Employees Admit To Bribing Amtrak Employee $320,000+ In Exchange For $50 Million+ Of Work - February 13, 2025

On or about December 10, 2015, a masonry restoration contractor was awarded a $58,473,000 contract by Amtrak to be the main contractor on a façade repair and restoration project at Amtrak's 30th Street Station in Philadelphia.

Federal funding supplied approximately 90 percent of the money Amtrak used to pay the cocntractor for the repair and restoration of the 30th Street Station façade.

Donald Seefeldt was the Senior Executive Vice President of the contractor with responsibility to provide executive oversight of the Contractor's performance on the 30th Street Station façade project.

Lee Maniatis and Khaled Dallo, both charged elsewhere, were Vice Presidents of the Contractor, with responsibility to supervise the contractor's performance on the 30th Street Station façade project.

Seefeldt and the others provided the Amtrak employee with gifts and other things of value totaling approximately $323,686, including, among other things, paid vacations, jewelry, cash, dinners, entertainment, and transportation, to ensure that the Amtrak employee used his power and influence to benefit the contractor during the performance of the 30th Street Station Repair and Restoration Project.

In return for these gifts and other things of value, the Amtrak employee used his position at Amtrak to access internal agency information available only to Amtrak employees about the 30th Street Station Project and shared this internal information with the defendant and other officials with the contractor. (Source)

Owner Of Accounting & Payroll Service Sentenced To Prison For Embezzling $344,000+ From Clients Over 5 Years To Repay Money She Had Stolen From Other Clients - February 24, 2024

Jeana McGowan, 58, owned and operated an accounting and payroll service headquartered in St. Louis Park, Minnesota, where she managed payroll for various small businesses. To facilitate the payroll service, - McGowan was granted access to client bank accounts.

On multiple occasions between 2016 and 2020, McGowan embezzled funds from her clients' bank accounts and used the money to cover personal expenses, or to pay back money she had previously embezzled from other clients. To accomplish her scheme, McGowan would electronically transfer funds from a client account into an account she controlled, in an amount appearing to be consistent with clients' payroll and spend the money for unapproved purposes. In total, she embezzled $344,813 from her clients over a period of five years.

On February 6, 2020, McGowan tried to cover her scheme by transferring money from an account she controlled and that had been funded with embezzled money into the account of another payroll client. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMENT AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

Company Finance Director Pleads Guilty To Embezzling $5.7 Million+ By Transfering Funds Into His Investment Account - February 5, 2025

Paul Schnitzer is the former Finance Director of a Florida based company.

Between January 2022 and May 2024, Schnitzer made more than 100 transfers out of his employer's operating bank account into an investment account he controlled, disguised as "equity distributions."

To hide these transfers, Schnitzer falsified financial reports to the Massachusetts-based investment firm that owned the company. Schnitzer also secretly used a line of credit to replenish the balance in the company's operating account after he had stolen from it. (Source)

Bookkeeper Sentenced To Prison For Stealing $1.6 Million+ From 2 Small Businesses / Used Funds For Luxury Apartment Rental, Car Payments, Shopping, Vacations - February 3, 2025

From 2016 to 2022, March Weiss (Age 50) engaged in a scheme to defraud two Mooresville, N.C. small businesses that employed him as a bookkeeper.

Over the course of the scheme, Weiss, who was a trusted employee, abused his position and access to the companies' financial accounts to make more than 100 fraudulent transfers totaling $1.6 million from the companies' accounts into bank accounts under Weiss's control. Court documents show that Weiss began to embezzle from the second company while he was already stealing from the first one. To disguise the fraud, Weiss created fake entries in the victim companies' books and records, categorizing the fraudulent transfers as payments to existing vendors for software development, and advertising and marketing expenses.

Weiss used the embezzled funds, in part, to pay for his personal lifestyle, including rent payments for a luxury apartment uptown; payments for high-end vehicles, including an Audi and a Mercedes-Benz; purchases at luxury retail stores, including Luis Vuitton, Gucci, Neiman Marcus, and Tiffany, among others; and luxury vacations, including multiple stays in The Ritz Carlton hotel. (Source)

Company Account Manager Sentenced To Prison For Stealing $1.1 Million+ From Employer / Used Funds For Vehicles, Jewelry, Etc. - February 21, 2025

Amy Shelton began working as an account manager for her employer in 2015. She was entrusted with handling payroll, paying bills, collecting rent, and updating financial documents.

From May 2019 through November 2022, Shelton wrote more than 150 checks to herself, totaling more than 1.1 million dollars. With those funds, Shelton purchased luxury items, including recreational vehicles, purses, jewelry, and dozens of firearms. Further, Shelton did not report her income accurately and falsified her tax refunds. Shelton was ordered to pay $870,934.67 in restitution to her former employer. (Source)

Water Authority Manager Sentenced To Prison For Stealing $1 Million+ By Diverting Money Into His Own Personal Bank Account - February 21, 2025

Michael Dominick was a former manager at the Ambridge Water Authority (AWA), where, during the period of January 2020 through August 2022, Dominick defrauded AWA of money and property totaling approximately $1,073,185.

As manager of AWA, Dominick was responsible for overseeing all daily business and financial activity and had access to AWA's bank accounts as well as cash and check payments made to AWA for water and related services.

Dominick secretly diverted AWA's money into his own personal bank accounts by writing checks to himself, depositing cash and checks issued to AWA into his personal bank accounts, using the AWA debit card to make purchases of personal items, and adjusting or failing to report the true location of AWA's funds on critical financial records. Dominick was ordered to pay restitution in the amount of $1,073,185. (Source)

Business Manager For Construction Company Charged With Embezzling $500,000+ From Employer / Used Funds To Pay Credit Cards, Travel, Etc. - February 10, 2025

Christina Mobley was employed as the business manager for a Fortuna Construction Company in California. When the company's bookkeeper retired, Mobley took on the accounting and bookkeeping duties, including inputting entries into the company's accounting software and assisting with bill payments, payroll taxes, employee health benefits, government contracts, and other tasks.

The company maintained an account at a bank and had several business credit cards through the bank for its employees. It also held a business credit card at another bank, where Mobley maintained at least two personal credit card accounts. The indictment describes that Mobley's scheme to defraud took on several forms. Mobley allegedly directed checks mailed from the company's bank account to be applied to the accounts for her personal credit cards; issued electronic payments of company funds to her personal credit cards; misused the company's credit card for personal expenses such as cash advances at casinos and personal travel; wrote checks

from the company to herself; inflated her vacation time, work hours, and bonuses in the company's payroll system; and issued duplicate payroll checks and unearned bonus payments to herself. Between January 2022 and November 2024, Mobley allegedly embezzled more than $500,000 from her employer. (Source)

Information Technology Manager For Non-Profit Organization Sentenced To Prison For Embezzling $360,000+ / Used Funds To Build House - February 28, 2025

From April 2015 to May 2020, Kyriakos Kapiris worked as the Information Technology Manager at Venture Community Services (VCS), a non-profit organization in Sturbridge, Mass. that services developmentally disabled members of the community. 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 to build a house. The house was forfeited by the government and sold. (Source)

Director Of Finance For Non-Profit Organization Admits To Embezzling $309,000 / Used Funds To Pay For Travel For Himself, Family, Friends - February 13, 2025

Jarrett Lewis was employed by the victim agency between June 2021 and October 2022.

While serving as Director of Finance for the non-profit, Lewis perpetrated a scheme to defraud his employer. Lewis was one of three employees with access to the non-profit's bank account. It was part of Lewis's duties to pay bills on behalf of the organization. Lewis was also provided with a VISA card for an account belonging to the organization, and was authorized to use the VISA card to incur expenses for goods and services related to its operations.

On 32 occasions, Lewis took advantage of his position by accessing the organizations account and causing funds to be transferred to his personal account and for his own personal benefit. The total loss suffered by Victim 1 resulting from these transfers is $309,950.88.

Lewis also used the non-profit's VISA to book and pay for personal travel for himself, his family, and friends, totaling $9,112. 96. In total, the parties stipulate that Lewis's scheme to defraud amounts to a total of $321,057.98. (Source)

Employee Admits Embezzling At Least $300,000 Over 5 Years By Manipulating The Human Resources Department / Used Funds For Travel & Friends - February 24, 2024

Scott Foster, 48, admitted as part of his plea that he committed the crime from January 2018 to December 2022, while employed as a mid-level executive of the company.

Foster manipulated the human resources systems to create an employee account for his paramour (Extramarital Partner), triggering wages and benefits totaling more than $273,000.00 to be paid to his paramour over nearly five years, despite this individual performing little or no actual work for the company.

Foster also used a corporate American Express card to pay for more than $33,000 in personal travel for himself, his paramour and other friends and acquaintances. (Source)

Former Employee Charged For Using Company Credit Card And Spending $260,000 To Purchase 150 Luxury Handbags - February 14, 2025

Kendra Gonzalez, while working as a comptroller is accused of using a company debit card to purchase 150 luxury handbags from a social commerce marketplace for online buying and selling of secondhand goods.

Gonzalez also allegedly used the company debit card for unauthorized personal expenses such as meals, entertainment, and hotel accommodations, and to send money to other people. (Source)

Office Manager For 3 Car Dealerships Sentenced to Prison For Embezzling $140,000 / Used Funds For Her Benefit - February 5, 2025

Beginning in September 2022 and continuing until February 2023, Madison Carrig, (30) Carrig was employed as the office manager of two automobile dealerships located in central Vermont. In that capacity, Carrig supervised all accounting activities at both dealerships.

Among other things, she had authority to sign checks, initiate wire transfers and make deposits to the dealerships' bank account. She also possessed a company credit card and was authorized to use the credit card to make business-related purchases.

Between February 2023 and November 27, 2023, Carrig was employed as the controller of a third Vermont automobile dealership, in Rutland. She had authority to sign checks, initiate wire transfers and make deposits to the dealership's bank account. She also possessed a company credit card and was authorized to use the credit card to make business-related purchases.

In the course of her employment, Carrig defrauded the three dealerships of approximately $140,000. She did this by embezzling cash receipts received from customers of the dealerships. She also misused company credit cards to purchase goods and services for her own use and benefit. (Source)

Office Manager Charged For Embezzling $100,000+ From Employer / Used Funds To Pay Credit Cards, Bills, Rent, Etc.- Fabruary 19, 2025

Victoria Isgriggs has been indicted and accused of embezzling more than $100,000 from her former employer.

Isgriggs, 44, worked at a nursery and florist as an office manager and accountant from approximately Nov. 26, 2023, through April 29, 2024. The indictment accuses Isgriggs of using a company bank account and company credit cards to pay personal expenses, including credit card debt, cell phone expenses, utility bills, and rent. The indictment also accuses Isgriggs of using company credit cards to make personal purchases that included luxury items and airfare. The indictment seeks the forfeiture of jewelry, Christian Louboutin footwear and Louis Vuitton bags and accessories. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE / UN-AUTHORIZED ACCESS TO COMPUTER SYSTEMS & NETWORKS

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Former Chinatown Walgreens Store Manager Pleads Guilty For Role On A Series Of Inside-Job Robberies - February 13, 2025

London Teeter and three co-conspirators devised a scheme to carry out armed robberies of the Walgreens store in Chinatown (Washington, DC) nearly once a month, beginning in July 2023, when either she or her co-conspirator were working.

As a store manager, Teeter knew the timing of cash transfers within the business.

In each robbery, a masked gunman entered the store, forced an employee into the manager's office or accessed the manager's office using a code provided by Teeter or her co-conspirator.

The gunman then robbed the employees and fled through a rear exit. Teeter and her co-conspirator took turns pretending to be the "victim" manager on duty, knowing that the robberies would be captured on internal surveillance.

In response to the robberies, the Chinatown Walgreens hired armed Special Police Officers to protect the business.

Teeter was aware that armed Special Police Officers would be present during the robberies and that a co-conspirator robbed the officers of their firearms during the robberies that occurred on December 4, 2023, and February 11, 2024.

Teeter admitted that the co-conspirators stole and split at least $28,983. She also acknowledged that she reviewed surveillance footage from the August 2, 2023, robbery during which a co-conspirator briefly placed his firearm on a chair Teeter acknowledged that she sent a co-conspirator a text message stating: "the vid looks so bad," "idk why he put the gun down," and "he can't do it next time [not gonna lie]." (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Hospital Emergency Room Nurse Charged For Stealing Fentanyl For Personal Use - February 6, 2025

While working as a registered nurse in the emergency room at Ascension St. John Hospital in Michigan, Travis Eskridge tampered with vials containing fentanyl, which he knew were intended to be administered to patients in the hospital's emergency room.

Eskridge removed fentanyl from the vials, replaced fentanyl with another liquid, and returned the tampered vials to the locked drug storage system. Eskridge did this with reckless disregard for the dangerous risk to patients that results from such tampering.

The indictment also charges that he stole fentanyl vials as part of a pattern of thefts over a nine-month period and obtained fentanyl by fraud for his personal use. Nurse Eskridge was removed from his position at Ascension St. John Hospital in August of 2022 when the tampering and thefts were discovered. (Source)

Hospital Nurse Pleads Guilty To Stealing Fentanyl For Her Own Use & Falsifying Hospital Records - February 21, 2025

On October 30, November 5 and 28, and December 3, 9, and 10, 2023, Lisa Williams, a Florida licensed registered nurse (RN), removed fentanyl from a secure drawer at the hospital.

Thereafter, Williams tampered with the fentanyl by removing a portion of the controlled substance from its container for her own personal use. After removing the fentanyl from the infusion bag, Williams swapped it with another container she had already tampered with and put it back into circulation. By tampering with the fentanyl, Williams acted with reckless disregard that the hospital patients would be placed in danger of death or bodily injury and under circumstances manifesting extreme indifference to such risk. Williams also knowingly manipulated the hospital records to falsely report a canceled transaction and give the fraudulent appearance that nothing was removed from the secure drawer. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Ohio Warehouse Shooting - 1 Killed, 5 Injured By Employee - February 5, 2025

Bruce Foster was apprehended after police executed a search warrant at an apartment in Columbus, Ohio, police said. Foster opened fire at a cosmetic manufacturing plant in New Albany, Ohio around 10:30 p.m. , police say.

The workplace shooting that left 1 person dead and 5 others wounded.

"He had been at work for some time when this occurred. We don't have any reports that there was any issue, that he was in an area that he wasn't supposed to be, or he was in trouble in any way or there was any conflict," New Albany Police Chief Greg Jones said. It is not to say there wasn't something, but after interviewing everybody we have, and the supervisor of the company we don't have any reports of anything like that. Jones earlier described the incident as a "targeted attack."

Foster has been charged with aggravated murder, according to Licking County court records. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & Other Sources) and be expanded.

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

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
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ 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' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ 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
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

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 (Pilots, Flight Attendants, Etc.)
  - 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, Etc.)
- ☐ 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 / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

IDEOLOGY

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

OTHER

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

They Have Used Company Funds / Credit Cards To Pay For:
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Grow Marijuana, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

They Have Issued Company Checks To:
Themselves, Family Members, Friends, Boyfriends / Girlfriends

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

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. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Key Findings From Report / Infographic
Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERE THE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

2 Former Employees Of Mortgage Lending Business Charged For Roles In $3 BILLION Mortgage Fraud Scheme - November 13, 2024

Christopher Gallo and Mehmet Ali Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business.

Gallo was a senior loan officer and Elmas was a mortgage loan officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties. By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than approximately $3 billion in loans. (Source)

TD Bank Pleads Guilty To Money Laundering Conspiracy By Bribed Employees / FINED $1.8 BILLION - October 10, 2024

TD Bank failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than $670 million through TD Bank accounts between 2019 and 2023.

Between January 2018 and February 2021, one money laundering network processed more than $470 million through the bank through large cash deposits into nominee accounts. The operators of this scheme provided employees gift cards worth more than $57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over $10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports.

In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million through shell accounts before TD Bank reported the activity.

In a third scheme, money laundering networks deposited funds in the United States and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately $39 million. The Justice Department has charged over two dozen individuals across these schemes, including two bank insiders. (Source)

Former Wells Fargo Executive Pleads Guilty To Opening Millions Of Accounts Without Customer Authorization - Wells Fargo Agrees To Pay $3 BILLION Penalty - March 15, 2023

The former head of Wells Fargo Bank's retail banking division (Carrie Tolstedt) has agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 BILLION penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding." (Source)

Former Company Chief Investment Officer Pleads Guilty To Role In $3 BILLION Of Securities Fraud / Company Pays $2.4 BILLION Fine - June 7, 2024

Gregorie Tournant is the former Chief Investment Officer and Co-Lead Portfolio Manager for a series of private investment funds managed by Allianz Global Investors (AGI).

Between 2014 and 2020, Tournant the Chief Investment Officer of a set of private funds at AGI known as the Structured Alpha Funds.

These funds were marketed largely to institutional investors, including pension funds for workers all across America. Tournant and his co-defendants misled these investors about the risk associated with their investments. To conceal the risk associated with how the Structured Alpha Funds were being managed, Tournant and his co-defendants provided investors with altered documents to hide the true riskiness of the funds' investments, including that investments were not sufficiently hedged against risks associated with a market crash.

In March 2020, following the onset of market declines brought on by the COVID-19 pandemic, the Structured Alpha Funds lost in excess of $7 Billion in market value, including over $3.2 billion in principal, faced margin calls and redemption requests, and ultimately were shut down.

On May 17, 2022, AGI pled guilty to securities fraud in connection with this fraudulent scheme and later was sentenced to a pay a criminal fine of approximately $2.3 billion, forfeit approximately $463 million, and pay more than $3 billion in restitution to the investor victims. (Source)

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Paying $1.6 BILLION In Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

Ng Chong Hwa, also known as "Roger Ng," a citizen of Malaysia and a former Managing Director of The Goldman Sachs Group, Inc., was was sentenced to 10 years in prisont for conspiring to launder BILLIONS of dollars embezzled from 1Malaysia Development Berhad (1MDB), conspiring to violate the Foreign Corrupt Practices Act (FCPA) by paying more than $1.6 BILLION in bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

1MDB is a Malaysian state-owned and controlled fund created to pursue investment and development projects for the economic benefit of Malaysia and its people.

Between approximately 2009 and 2014, Ng conspired with others to launder billions of dollars misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions it executed with Goldman Sachs, known as "Project Magnolia," "Project Maximus," and "Project Catalyze." As part of the scheme, Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite also known as "Jho Low," conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

They also conspired to launder the proceeds of their criminal conduct through the U.S. financial system by funding major Hollywood films such as "The Wolf of Wall Street," and purchasing, among other things, artwork from New York-based Christie's auction house including a $51 million Jean-Michael Basquiat painting, a $23 million diamond necklace, millions of dollars in Hermes handbags from a dealer based on Long Island, and luxury real estate in Manhattan.

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

Boeing Charged With 737 Max Fraud Conspiracy Agrees To Pay Over $2.5 BILLION In Penalties Because Of Employees Fraudulent And Deceptive Conduct - January 11, 2021

Aircraft manufacturer Boeing has agreed to pay over $2.5 billion in penalties as a result of "fraudulent and deceptive conduct by employees" in connection with the firm's B737 Max aircraft crashes.

"The misleading statements, half-truths, and omissions communicated by Boeing employees to the FAA impeded the government's ability to ensure the safety of the flying public," said U.S. Attorney Erin Nealy Cox for the Northern District of Texas.

As Boeing admitted in court documents, Boeing through two of its 737 MAX Flight Technical Pilots deceived the FAA about an important aircraft part called the Maneuvering Characteristics Augmentation System (MCAS) that impacted the flight control system of the Boeing 737 MAX. Because of their deception, a key document published by the FAA lacked information about MCAS, and in turn, airplane manuals and pilot-training materials for U.S.-based airlines lacked information about MCAS.

On Oct. 29, 2018, Lion Air Flight 610, a Boeing 737 MAX, crashed shortly after takeoff into the Java Sea near Indonesia. All 189 passengers and crew on board died.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 MAX, crashed shortly after takeoff near Ejere, Ethiopia. All 157 passengers and crew on board died. (Source)

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than $1.4 billion in loans. (Source)

Member Of Supervisory Board Of State Employees Federal Credit Union Pleads Guilty To $1 BILLION Scheme Involving High Risk Cash Transactions - January 31, 2024

A New York man pleaded guilty today to failure to maintain an anti-money laundering program in violation of the Bank Secrecy Act as part of a scheme to bring lucrative and high-risk international financial business to a small, unsophisticated credit union.

From 2014 to 2016, Gyanendra Asre of New York, was a member of the supervisory board of the New York State Employees Federal Credit Union (NYSEFCU), a financial institution that was required to have an anti-money laundering program. Through the NYSEFCU and other entities, Asre participated in a scheme that brought over $1 billion in high-risk transactions, including millions of dollars of bulk cash transactions from a foreign bank, to the NYSEFCU.

In addition, Asre was a certified anti-money laundering specialist who was experienced in international banking and trained in anti-money laundering compliance and procedures, and represented to the NYSEFCU that he and his businesses would conduct appropriate anti-money laundering oversight as required by the Bank Secrecy Act. Based on Asre's representations, the NYSEFCU, a small credit union with a volunteer board that primarily served New York state public employees, allowed Asre and his entities to conduct high-risk transactions through the NYSEFCU. Contrary to his representations, Asre willfully failed to implement and maintain an anti-money laundering program at the NYSEFCU. This failure caused the NYSEFCU to process the high-risk transactions without appropriate oversight and without ever filing a single Suspicious Activity Report, as required by law. (Source)

Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024

3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the world. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Pearce concealed the fraud scheme for many years by using these privileges to alter information about the accounts, which helped hide his creation of unauthorized license keys. Dusti Pearce handled accounting for the illegal business.

Hines operated Direct Business Services International (DBSI), a New Jersey-based business communications systems provider and a de-authorized Avaya reseller. He bought ADI software license keys from Brad and Dusti Pearce and then sold them to resellers and end users around the world for significantly below the wholesale price. Hines was by far the Pearces' largest customer and significantly influenced how the scheme operated. Hines was one of the biggest users of the ADI license system in the world.

To hide the nature and source of the money, the Pearces funneled their illegal gains through a PayPal account created under a false name to multiple bank accounts, and then transferred the money to investment and bank accounts. They also purchased large quantities of gold bullion and other valuable items. (Source)

COLLUSION – HOW MANY EMPLOYEES' OR INDIVIDUALS CAN BE INVLOVED?

193 Individuals Charged (Doctors, Nurses, Medical Professionals) For Participation In $2.75 BILLION Health Care Fraud Schemes - June 27, 2024

The Justice Department today announced the 2024 National Health Care Fraud Enforcement Action, which resulted in criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

In connection with the coordinated nationwide law enforcement action, and together with federal and state law enforcement partners, the government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication; over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

2 Executives Who Worked For a Geneva Oil Production Firm Involved In Misappropriating $1.8 BILLION - April 25, 2023

The former Petrosaudi employees are suspected of having worked with Jho Low, the alleged mastermind behind the scheme, to set up a fraudulent deal purported between the governments of Saudi Arabia and Malaysia, according to a statement from the Swiss Attorney General.

1MDB was the Malaysian sovereign wealth fund designed to finance economic development projects across the southeastern Asian nation but become a byword for scandal and corruption that triggered investigations in the US, UK, Singapore, Malaysia, Switzerland and Canada.

Low, currently a fugitive whose whereabouts are unknown, has previously denied wrongdoing. His playboy lifestyle was financed with money stolen from 1MDB, according to US prosecutors.

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 billion in financing from 1MDB, according to Swiss prosecutors. The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

The allegations cover a period at least from 2009 to 2015 and the duo have been indicted for commercial fraud, aggravated criminal mismanagement and aggravated money laundering. (Source)

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION in Health Care Fraud Scheme - June 28, 2023

The Justice Department, together with federal and state law enforcement partners, announced today a strategically coordinated, two-week nationwide law enforcement action that resulted in criminal charges against 78 defendants for their alleged participation in health care fraud and opioid abuse schemes that included over $2.5 Billion in alleged fraud. The enforcement action included charges against 11 defendants in connection with the submission of over $2 Billion in fraudulent claims resulting from telemedicine schemes.

In a case involving the alleged organizers of one of the largest health care fraud schemes ever prosecuted, an indictment in the Southern District of Florida alleges that the Chief Executive Officer (CEO), former CEO, and Vice President of Business Development of purported software and services companies conspired to generate and sell templated doctors' orders for orthotic braces and pain creams in exchange for kickbacks and bribes. The conspiracy allegedly resulted in the submission of $1.9 Billion in false and fraudulent claims to Medicare and other government insurers for orthotic braces, prescription skin creams, and other items that were medically unnecessary and ineligible for Medicare reimbursement. (Source)

10 Individuals (Hospital Managers And Others) Charged In $1.4 BILLION Hospital Pass - Through Billing Scheme - June 29, 2020

10 individuals, including hospital managers, laboratory owners, billers and recruiters, were charged for their participation in an elaborate pass-through billing scheme using rural hospitals in several states as billing shells to submit fraudulent claims for laboratory testing.

The indictment alleges that from approximately November 2015 through February 2018, the conspirators billed private insurance companies approximately $1.4 billion for laboratory testing claims as part of this fraudulent scheme, and were paid approximately $400 million. (Source)

Former University Financial Advisor Sentenced To Prison For $5.6 Million+ Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee.

As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied.

Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

3 Bank Board Members Of Failed Bank Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman.

Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

TRADE SECRET THEFT

Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION - May 2, 2022

Gongda Xue worked as a scientist at the Friedrich Miescher Institute for Biomedical Research (FMI) in Switzerland, which is affiliated with Novartis. His sister, Yu Xue, worked as a scientist at GlaxoSmithKline (GSK) in Pennsylvania. Both Gongda Xue and Yu Xue conducted cancer research as part of their employment at these companies.

While working for their respective entities, Gongda Xue and Yu Xue shared confidential information for their own personal benefit.

Gongda Xue created Abba Therapeutics AG in Switzerland, and Yu Xue and her associates formed Renopharma, Ltd., in China. Both companies intended to develop their own biopharmaceutical anti-cancer products.

Gongda Xue stole FMI research into anti-cancer products and sent that research to Yu Xue. Yu Xue, in turn, stole GSK research into anti-cancer products and sent that to Gongda Xue. Yu Xue also provided hundreds of GSK documents to her associates at Renopharma. Renopharma then attempted to re-brand GSK products under development as Renopharma products and attempted to sell them for billions of dollars. Renopharma's own internal projections showed that the company could be worth as much as $10 billion based upon the stolen GSK data. (Source)

U.S. Brokerage Firm Accuses Rival Firm Of Stealing Trade Secrets Valued At Over $1 BILLION - November 14, 2023

U.S. brokerage firm BTIG sued rival StoneX Group, accusing it of stealing trade secrets and seeking at least $200 million in damages.

StoneX recruited a team of BTIG traders and software engineers to exfiltrate BTIG software code and proprietary information and take it to StoneX, according to lawyers for BTIG.

StoneX used the software code and proprietary information to build competing products and business lines that generate tens of millions of dollars annually, they alleged in the lawsuit.

BTIG said in the lawsuit that StoneX had committed one of the greatest financial industry trade secret frauds in recent history, and that the scope of its misconduct is not presently known, and may easily exceed a billion dollars."

The complaint said StoneX hired several BTIG employees to steal confidential information that it used to develop its competing trading platform.

The complaint said that StoneX's stock price has increased 60% since it started misusing BTIG's trade secrets. (Source)

U.S. Petroleum Company Scientist Sentenced To Prison For $1 BILLION Theft Of Trade Secrets - Was Starting New Job In China - May 27, 2020

When scientist Hongjin Tan resigned from the petroleum company he had worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.

But Tan told a colleague a different story over dinner. He revealed to his colleague that he actually did have a job waiting for him in China. Tan's dinner companion reported the conversation to his supervisor. That conversation prompted Tan's employer to ask him to leave the firm immediately, and his employer made a call to the FBI tip line to report a possible crime.

Tan called his supervisor to tell them he had a thumb drive with company documents on it. The company told him to return the thumb drive. When he brought back the thumb drive, the company looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about. (Source)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners.

As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

CEO Of Bank Sentenced To Prison For $47 Million Fraud Scheme That Caused Bank To Collapse - August 19, 2024

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering."

The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (Source)

3 Bank Board Members Of Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged / Bank Collapsed - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (Source)

Bank Director Convicted For $1.4 Million Of Bank Fraud Causing Bank To Collapse - July 12, 2023

In 2009, Mendel Zilberberg (Bank Director) conspired with Aron Fried and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower (Straw Borrower) to make the loan application. The Straw Borrower applied for a $1.4 Million loan from the Bank on the basis of numerous lies directed by Zilberberg and his coconspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly.

Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a $1.4 Million loan to the Straw Borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately $500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator.

The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. (Source)

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 Role in $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)

EMPLOYEE EXTORTION

Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / He Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - February 2, 2023

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through April 1, 2021. Sharp was a Senior Developer who had administrative to credentials for company's Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from his technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guilty To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022

Casey Umetsu worked as an Information Technology Professional for a prominent Hawaii-based financial company between 2017 and 2019. In that role, Umetsu was responsible for administering the company's computer network and assisting other employees' with computer and technology problems.

Umetsu admitted that, shortly after severing all ties with the company, he accessed a website the company used to manage its internet domain. After using his former employer's credentials to access the company's configuration settings on that website, Umetsu made numerous changes, including purposefully misdirecting web and email traffic to computers unaffiliated with the company, thereby incapacitating the company's web presence and email. Umetsu then prolonged the outage for several days by taking a variety of steps to keep the company locked out of the website. Umetsu admitted he caused the damage as part of a scheme to convince the company it should hire him back at a higher salary. (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)

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)

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (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)

Fired IT System Administrator Sabotages Railway Network - February 14, 2018

Christopher Grupe was suspended for 12 days back in December 2015 for insubordination while working for the Canadian Pacific Railway (CPR). When he returned the CPR had already decided they no longer wanted to work with Grupe and fired him. Grupe argued and got them to agree to let him resign. Little did CPR know, Grupe had no intention of going quietly.

As an IT System Administrator, Grupe had in his possession a work laptop, remote access authentication token, and access badge. Before returning these, he decided to sabotage the railway's computer network. Logging into the system using his still-active credentials, Grupe removed admin-level access from other accounts, deleted important files from the network, and changed passwords so other employees' could no longer gain access. He also deleted any logs showing what he had done.

The laptop was then returned, Grupe left, and all hell broke loose. Other CPR employees' couldn't log into the computer network and the system quickly stopped working. The fix involved rebooting the network and performing the equivalent of a factory reset to regain access.

Grupe may have been smirking to himself knowing what was going on, but CPR's management decided to find out exactly what happened. They called in computer forensic experts who found the evidence needed to prosecute Grupe. Grupe was found guilty of carrying out the network sabotage and handed a 366 day prison term. (Source)

Former IT Systems Administrator Sentenced To Prison For Hacking Computer Systems Of His Former Employer - Causing Company To Go Out Of Business (2010)

Dariusz Prugar worked as a IT Systems Administrator for an Internet Service Provider (Pa Online) until June 2010. But after a series of personal issues, he was let go.

Prugar logged into PA Online's network, using his old username and password. With his network privileges he was able to install backdoors and retrieve code that he had been working on while employed at the ISP.

Prugar tried to cover his tracks, running a script that deleted logs, but this caused the ISP's systems to crash, impacting 500 businesses and over 5,000 residential customers of PA Online, causing them to lose access to the internet and their email accounts.

According to court documents, that could have had some pretty serious consequences: "Some of the customers were involved in the transportation of hazardous materials as well as the online distribution of pharmaceuticals."

Unaware that Prugar was responsible for the damage, PA Online contacted their former employee requesting his help. However, when Prugar requested the rights to software and scripts he had created while working at the firm in lieu of payment. Pa Online got suspicious and called in the FBI.

A third-party contractor was hired to fix the problem, but the damage to PA Online's reputation was done and the ISP lost multiple clients.

Prugar ultimately pleaded guilty to computer hacking and wire fraud charges, and received a two year prison sentence alongside a $26,000 fine.

And PA Online? Well, they went out of business in October 2015. (Source)

Former IT Administrator Sentenced To Prison For Attempting Computer Sabotage On 70 Company Servers / Feared He Was Going To Be Laid Off (2005)

Yung-Hsun Lin was a former Unix System Administrator at Medco Health Solutions Inc.'s Fair Lawn, N.J. He pleaded guilty in federal court to attempting to sabotage critical data, including individual prescription drug data, on more than 70 servers.

Lin was one of several systems administrators at Medco who feared they would get laid off when their company was being spun off from drug maker Merck & Co. in 2003, according to a statement released by federal law enforcement authorities. Apparently angered by the prospect of losing his job, Lin on Oct. 2, 2003, created a "logic bomb" by modifying existing computer code and inserting new code into Medco's servers.

The bomb was originally set to go off on April 23, 2004, on Lin's birthday. When it failed to deploy because of a programming error, Lin reset the logic bomb to deploy on April 23, 2005, despite the fact that he had not been laid off as feared. The bomb was discovered and neutralized in early January 2005, after it was discovered by a Medco computer systems administrator investigating a system error.

Had it gone off as scheduled, the malicious code would have wiped out data stored on 70 servers. Among the databases that would have been affected was a critical one that maintained patient-specific drug interaction information that pharmacists use to determine whether conflicts exist among an individual's prescribed drugs. Also affected would have been information on clinical analyses, rebate applications, billing, new prescription call-ins from doctors, coverage determination applications and employee payroll data. (Source)

Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System - September 26, 2014

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

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

Lottery Official Tried To Rig $14 Million+ Jackpot By Inserting Software Code Into Computer That Picked Numbers - Largest Lottery Fraud In U.S. History - 2010

This incident happened in 2010, but the articles on the links below are worth reading, and are great examples of all the indicators that were ignored.

Eddie Tipton was a Lottery Official in Iowa. Tipton had been working for the Des Moines based Multi-State Lottery Association (MSLA) since 2003, and was promoted to the Information Security Director in 2013.

Tipton was first convicted in October 2015 of rigging a $14.3 Million drawing of the MSLA lottery game Hot Lotto. Tipton never got his hands on the winning total, but was sentenced to prison. Tipton was released on parole in July 2022.

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005.

Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

That software code was replicated on as many as 17 state lottery systems, as the MSLA random-number software was designed by Tipton. For nearly a decade, it allowed Tipton to rig the drawings for games played on three dates each year: May 27, Nov. 23 and Dec. 29.

Tipton ultimately confessed to rigging other lottery drawings in Colorado, Wisconsin, Kansas and Oklahoma.

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

Eddie Tipton was making almost $100,000 a year. But he felt underappreciated and overworked at the time he wrote the code to hack into the national lottery system.

He was working 50- to 60-hour weeks and often was in the office until 11 p.m. His managers expected him to take on far more roles than were practical, he complained.

Tipton Stated: "I wrote software. I worked on Web pages. I did network security. I did firewalls," he said in his confession. "And then I did my regular auditing job on top of all that. They just found no limits to what they wanted to make me do. It even got to the point where the word ‘slave’ was used."

Nobody at the MSLA oversaw his complete body of work, and few people truly cared about security, he said. That lack of oversight allowed Tipton to write, install and use his secret code without discovery.
Video Complete Story Indicators Overlooked / Ignored

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021

On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank’s boardroom however the entire bank suffered smoke damage.

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day.

The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

She also admitted to using the fraudulently obtained money to fund her boyfriend's business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million dollars. (Source)

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023
Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

Cook was fired for being intoxicated at work. She returned shortly after being escorted out of the hotel by police and set multiple fires in the hotel, displacing the occupants of more than 400 rooms. (Source)

WORKPLACE VIOLENCE
Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024
Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

Between May and August 2022, numerous patients at Surgicare North Dallas suffered cardiac emergencies during routine medical procedures performed by various doctors. About one month after the unexplained emergencies began, an anesthesiologist who had worked at the facility earlier that day died while treating herself for dehydration using an IV bag. In August 2022, doctors at the surgical care center began to suspect tainted IV bags had caused the repeated crises after an 18-year-old patient had to be rushed to the intensive care unit in critical condition during a routine sinus surgery.

A local lab analyzed fluid from the bag used during the teenager's surgery and found bupivacaine (a nerve-blocking agent), epinephrine (a stimulant) and lidocaine (an anesthetic) — a drug cocktail that could have caused the boy's symptoms, which included very high blood pressure, cardiac dysfunction and pulmonary edema. The lab also observed a puncture in the bag.

Ortiz surreptitiously injected IV bags of saline with epinephrine, bupivacaine and other drugs, placed them into a warming bin at the facility, and waited for them to be used in colleagues' surgeries, knowing their patients would experience dangerous complications. Surveillance video introduced into evidence showed Ortiz repeatedly retrieving IV bags from the warming bin and replacing them shortly thereafter, not long before the bags were carried into operating rooms where patients experienced complications. Video also showed Ortiz mixing vials of medication and watching as victims were wheeled out by emergency responders.

Evidence presented at trial showed that Ortiz was facing disciplinary action at the time for an alleged medical mistake made in his one of his own surgeries, and that he potentially faced losing his medical license. (Source)

Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022

A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

A jury initially awarded more than $7 billion in damages in July, but the judge lowered that number to roughly $1.1 Billion.

Roy Holden, the former employee who murdered Thomas, performed a service call at her home in December 2019. The next day, while off-duty, he went back to her house and stole her credit cards as he was fixing her fax machine, then stabbed her to death before going on a spending spree with the stolen cards.

The attorneys also argued that Charter Spectrum hired Holden without reviewing his work history and ignored red flags during his employment. (Source) (Source)

Former Nurse Charged With Murder Of 2 Patients At Hospital, Nearly Killing 3rd By Administering Lethal Doses Of Insulin - October 26, 2022

Jonathan Hayes, a 47-year-old former Nurse at Atrium Health Wake Forest Baptist Medical Center in Winston-Salem, North Carolina, has been charged with 2 counts of murder and 1 count of attempted murder.

O'Neill said that on March 21, a team of investigators at the hospital presented him with information that Hayes may have administered a lethal dose of insulin to one patient and indicated there may be other victims.

The 1 count of murder against Hayes is related to the death of 61 year old Jen Crawford. Hayes administered a lethal dose of insulin to Crawford on Jan. 5. She died three days later.

The 2 count of murder is in connection with the death of 62-year-old Vickie Lingerfelt, who was administered a lethal dose of insulin on Jan. 22. She died on Jan. 27.

Hayes is also charged with administering a near-lethal dose of insulin to 62-year-old Pamela Little on Dec. 1, 2021. Little survived and Hayes faces one count of attempted murder.

Hayes was terminated from the hospital in March 2022, and he was arrested In October 2022. (Source)

Hospital Nurse Alleged Killer Of 7 Babies / 15 Attempted Murders - October 13, 2022

A neonatal nurse in the U.K. who allegedly murdered 7 babies and attempted to kill 10 more wrote notes reading, "I don't deserve to live," "I killed them on purpose because I'm not good enough to care for them. I am a horrible evil person."

Lucy Letby, 32, who worked in the Neonatal Unit of the Countess of Chester Hospital, left handwritten notes in her home that police found when they searched it in 2018, prosecutor Nick Johnson stated during her trial in October 2022.

Johnson argued that Letby was a constant, malevolent presence in the neonatal unit. Of the babies Letby allegedly murdered or attempted to murder between 2015 and 2016, the prosecution said she injected some with insulin or milk, while another she injected with air. She allegedly attempted to kill one baby three times.

Johnson told jurors the hospital had been marked by a significant rise in the number of babies who were dying and in the number of serious catastrophic collapses" after January 2015, before which he said its rates of infant mortality were comparable to other busy hospitals.

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours.

Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

Former Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans - May 11, 2021

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VAMC) in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

Indianapolis FedEx Shooter That Killed 8 People Was Former FedEx Employee With Mental Health Problems - April 20, 2021

Police say the 19 year old Indianapolis man who fatally shot 8 people at a southwest side FedEx Ground facility in April had planned the attack for at least nine months.

In a press conference, local and federal officials said the shooting was "an act of suicidal murder" in which Bandon Scott Hole decided to kill himself "in a way he believed would demonstrate his masculinity and capability while fulfilling a final desire to experience killing people."

Hole worked at the FedEx facility between August and October 2020. Police believe he targeted his former workplace not because he was trying to right a perceived injustice, but because he was familiar with the "pattern of activity" at the site.

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house.

Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check.

Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

Former Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder - September 22, 2020

On August 12, 2003, Richard Wilbern walked into Xerox Federal Credit Union, located on the Xerox Corporation campus, and committed robbery and murder. Wilbern was not caught until 2016 for robbery and murder, and was sentenced this week to life in prison.

Richard Wilbern walked into Xerox Federal Credit Union (XFCU) and was wearing a dark blue nylon jacket with the letters FBI written in yellow on the back of the jacket, sunglasses and a poorly fitting wig. Wilbern was also carrying a large briefcase, a green and gray-colored umbrella and had what appeared to be a United States Marshals badge hanging on a chain around his neck.

Wilbern was employed by Xerox between September 1996 and February 23, 2001 as which time he was terminated for repeated employment related infractions. In 2001, Wilbern filed a lawsuit against Xerox alleging that the company unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. Wilbern also maintained a checking and savings accounts at the Xerox Federal Credit Union. Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy.

In March 2016, a press conference was held to seek new leads in the investigation. Details of the crime were released as well as photographs of Wilbern committing the robbery. Anyone with information was asked to call a dedicated hotline.

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

In July 20016, FBI agents met with Wilbern regarding a complaint he had made to the FBI regarding an alleged real estate scam. During one of their meetings, agents obtained a DNA sample from Wilbern after he licked and sealed an envelope. That envelope was sent to OCME, and after comparing the DNA profile from the envelope to the DNA profile previously developed from the umbrella, determined there was a positive match. (Source)

Florida Best Buy Driver Murders 75 Year Old Woman While Delivering Her Appliances - Lawyers Said The Murder Was Preventable If Best Buy Had Better Screened Employees' - September 30, 2019

A Boca Raton family has filed a wrongful death lawsuit against Best Buy. This comes after allegations a delivery man for the company killed a 75-year-old woman while delivering appliances.

The family of 75 year old Evelyn Udell has filed a wrongful death lawsuit to hold Best Buy, two delivery contractors and the two deliverymen, accountable for her death.

Lawyers say the fatal attack was preventable if the companies had further screened their employees'.

On August 19th, police say Jorge Lachazo and another man were delivering a washer and dryer the Udells had bought from Best Buy.

Police say Lachazo beat Udell with a mallet, poured acetone on her body and set her on fire. She died the next day. Lachazo was arrested and is charged with murder.

According to the lawsuit, Best buy stores did nothing to investigate, supervise, or oversee the personnel used to perform these services on their behalf. Worse, it did nothing to advise, inform, or warn Mrs. Udell that the delivery and installation services had been delegated to a third-party.

Lawyers are also calling for sweeping changes to how businesses screen workers who have to go inside a customers' home. (Source)

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE
This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

View On The Link Below Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

CTTP = China Thousand Talents Plan

- NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers
- U.S. Petroleum Company Scientist STP For $1 Billion Theft Of Trade Secrets - Was Starting New Job In China
- Cleveland Clinic Doctor Arrested For $3.6 Million Grant Funding Fraud Scheme Involving CTTP
- Hospital Researcher STP For Conspiring To Steal Trade Secrets And Sell Them in China With Help Of Husband
- Employee Of Research Institute Pleads Guilty To Steal Trade Secrets To Sell Them In China
- Raytheon Engineer STP For Exporting Sensitive Military Technology To China
- GE Power & Water Employee Charged With Stealing Turbine Technologies Trade Secrets Using Steganography For Data Exfiltration To Benefit People's Republic of China
- CIA Officer Charged With Espionage Over 10 Years Involving People's Republic of China
- Massachusetts Institute of Technology (MIT) Professor Charged With Grant Fraud Involving CTTP
- Employee At Los Alamos National Laboratory Receives Probation For Making False Statements About Being Employed By CTTP
- Texas A&M University Professor Arrested For Concealing His Association With CTTP
- West Virginia University Professor STP For Fraud And Participation In CTTP
- Harvard University Professor Charged With Receiving Financial Support From CTTP
- Visiting Chinese Professor At University of Texas Pleads Guilty To Lying To FBI About Stealing American Technology
- Researcher Who Worked At Nationwide Children's Hospital's Research Institute For 10 Years, Pleads Guilty To Stealing Scientific Trade Secrets To Sell To China
- U.S. University Researcher Charged With Illegally Using $4.1 Million In U.S. Grant Funds To Develop Scientific Expertise For China
- U.S. University Researcher Charged With VISA Fraud And Concealed Her Membership In Chinese Military
- Chinese Citizen Who Worked For U.S. Company Convicted Of Economic Espionage, Theft Of Trade Secrets To Start New Business In China
- Tennessee University Researcher Who Was Receiving Funding From NASA Arrested For Hiding Affiliation With A Chinese University
- Engineers Found Guilty Of Stealing Micron Secrets For China
- Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China
- Husband And Wife Scientists Working For American Pharmaceutical Company, Plead Guilty To Illegally Importing Potentially Toxic Lab Chemicals And Illegally Forwarding Confidential Vaccine Research to China
- Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Setup New Business In China
- Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION To Setup Business In China
- University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government
- Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company
- Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees' To Steal Technology

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy
- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**6,000+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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 / X

Updated Daily

https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.

https://www.nationalinsiderthreatsig.org/aboutnitsig.html

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage, evaluate and optimize an Insider Risk Management (IRM) Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates, as well as attended our Insider Threat Investigations - Analysis Training Course and other training courses.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and IRM Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive IRM.

ITDG training and consulting services will empower individuals that manage or support IRM Programs, with the comprehensive knowledge, tools and a unified and holistic approach to identify, prevent and mitigate Insider Risks / Threats.

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED
Conducted Via Classroom / Onsite / Web Based
TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Development, Management & Optimization Training Course
- ✓ IRM Program Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of 675 Clients:
White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Members
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org