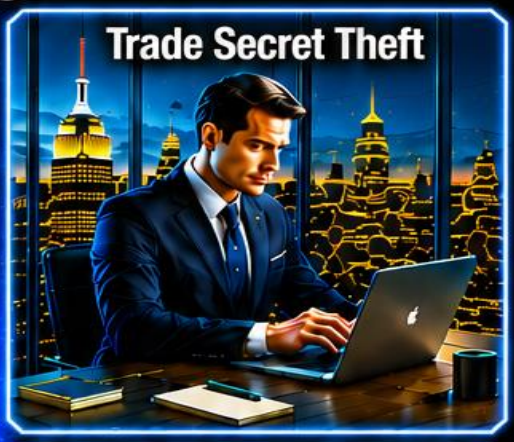
INSIDER THREAT INCIDENTS REPORT FOR

★ August 2026 ★



DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM

Produced By

National Insider Threat Special Interest Group

★

Insider Threat Defense Group

TABLE OF CONTENTS

INSIDER THREAT INCIDENTS OVERVIEW

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 **7,400+** 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 is very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

Additional insights into the increase in fraud is outlined on pages 39 to 44 of this report, providing results from the Association of Certified Fraud Examiners 2026 Report To the Nations.

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 hundreds of thousands of dollars, maybe millions 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 32** 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 AUGUST 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
Australian Institute Of Insider Threats - Insider Threat Incidents Weekly Reports
https://www.insiderthreats.au/threat-warning

Canadian Intern At NATO Military HQ Arrested On Spying Charge - July 25, 2026
A Canadian woman of Chinese origin who was an intern at NATO's military headquarters in Belgium has been arrested on spying charges, Belgian prosecutors said. "She is suspected of spying on behalf of a third country and of being a member of a criminal organization," the Federal Public Prosecutor's Office said in a statement.

The woman worked as an intern at NATO's Supreme Headquarters Allied Powers Europe (SHAPE) in the Belgian city of Mons, the statement said. It did not provide further details of her identity or the country or organization she is suspected of spying for.

SHAPE is NATO's top military headquarters, the base of Allied Command Operations, which is responsible for planning and carrying out all operations of the 32-member transatlantic security alliance.
The suspect had come to the attention of SHAPE's security services, who reported her to Belgian intelligence officials, according to the prosecutors' statement. Investigators searched the suspect's home and her workplace at SHAPE, and she was placed under arrest on Friday. A SHAPE spokesperson said there was no indication that NATO or SHAPE operational readiness, command and control arrangements or ongoing tasks had been affected. (Source)

Senior Engineer Charged In Taiwan For Stealing DRAM Trade Secrets Using Hidden Camera - August 15, 2026
A senior engineer at Nanya Technology has been indicted in Taiwan for allegedly copying 32 files containing information about the company's DRAM manufacturing process, reports Freedom Times. The engineer was reportedly in talks with Chinese recruitment agencies and allegedly planned to pass Nanya's trade secrets to its next employer in the People's Republic in exchange for higher compensation.

Yeh Yen-wei, a senior engineer in the Advanced Process Development Division at Nanya, joined the company in 2022 and began to communicate with Chinese recruiters in 2025 to explore employment opportunities in the People's Republic. Sometime in mid-February 2026, he submitted his resignation. However, before leaving the company in mid-April, on March 28, April 4, and April 5 — during weekends and either late at night or early in the morning — he visited the company's restricted office areas with his Insta360 X4 Air action camera hidden among snacks to get it past security checks. (Source)

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES
No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS
No Incidents To Report

U.S. GOVERNMENT

3 U.S. Postal Service Employees & Resident Charged With Stealing $24 Million Worth Of Checks From Mail - August 25, 2026

Tryston Vaughn, 28, Malcolm Joubert, 35, Alyssa Bryant, 27, Catherine Kilpatrick, 29, and Drakkor Alexander, 34 are being charged in this incident.

Vaughn allegedly recruited U.S. Postal Service mail carriers to steal checks from the mail along their routes. Vaughn and others allegedly purchased the stolen checks from postal employees and resold them to buyers through Telegram. They then shipped the stolen checks to buyers, according to the indictment.

Kilpatrick, Joubert, and Alexander worked as USPS mail carriers when Vaughn allegedly recruited them to steal mail. (Source)

U.S. Mail Carrier Sentenced To Prison For Stealing $1 Million+ Of Checks From Mail - - August 25, 2026

From August 2022 to September 2024, Melissa McAfee,44, worked as a U.S. Postal Service mail carrier in the Smyrna, Georgia area.

The U.S. Postal Service - Office of Inspector General (USPS-OIG) launched an investigation after receiving customer complaints about mail stolen along McAfee's postal route. During the investigation, USPS-OIG obtained surveillance footage of McAfee stealing mail on her route. Additional investigation determined that she stole mail containing 171 checks, with a total value exceeding $1,035,000. USPS-OIG agents executed a search warrant at McAfee's home, where they discovered envelopes for stolen mail, 145 stolen checks, and 37 stolen gift cards. When confronted by USPS-OIG agents in September 2024, McAfee resigned from the Postal Service. (Source)

U.S Postal Service Employee Pleads Guilty To Attempting To Destroy 498 Of Pieces Mail Instead Of Delivering - August 4, 2024

Stacy Braxton, 39, was a rural mail carrier for the Greenwood Post Office in Jackson County, Florida. In February 2026, law enforcement recovered 498 pieces of mail from the defendant's mail route that were discarded in a burn barrel in Marianna, Florida. The defendant admitted to investigators that she attempted to discard and burn the mail from her route rather than delivering the mail to the designated recipients. (Source)

U.S. Postal Service Employee Pleads Guilty To Embezzling $26,700 - August 28, 2026

In January 2025, the U.S, Postal Service determined the post office in Quinter, Kansas, had a significant shortfall. The deficit was in missing deposits, deposit short in cash, errors on bank deposits, and money orders issued and voided on the same day but negotiated after being voided.

An investigation revealed Sierra Werth, 32 issued and voided at least 10 money orders on the same day. She issued seven money orders under her employee ID and included her name and address in the remitter section. There were three money orders issued under a different postal employee's ID, but they had her name and address in the remitter section. Also, the name of someone associated with Werth was in the "pay to" section of the all the money orders. The records show the money orders were issued, voided, and cashed without USPS receiving payment, and that Werth had engaged in this activity since approximately October 2024. Law enforcement found an additional invoice the Werth created. As part of her plea agreement, Werth must pay approximately $26,700 in restitution. (Source)

USDA Program Director Sentenced To Prison For $399,000+ Fraud Scheme Involving Nephew - August 7, 2026

Kirk Perry, 62, a former United States Department of Agriculture (USDA) program director, was sentenced today to 24 months in prison in connection with a kickback scheme in which he and his nephew, Jamarea Grant, 32, conspired to bill the government for $399,319 of work that Grant did not actually perform.

Perry was a senior director within the USDA's Office of the Assistant Secretary for Civil Rights and used his position to secure employment for Grant as an Equal Opportunity Assistant.

In pleading guilty, Perry and Grant admitted that, from August 2015 through November 2022, Perry arranged for Grant to be hired by two companies under contract with the USDA Office of Assistant Secretary for Civil Rights. Grant reported directly to Perry, who also approved the invoices billing for Grant's time, and the two of them conspired to bill the government for work that Grant did not perform.

Perry additionally had access to Grant's bank account. As part of the criminal scheme, Perry transferred approximately $125,000 of the USDA payments from Grant's account to his own account. Grant's sentencing is pending. (Source)

Department Of Labor Employee Sentenced To Prison For Fraudulently Obtaining $40,000+ In Covid Pandemic Unemployment Assistance Benefits - August 11, 2026

Mo Yuong Kang, 51, worked as an Industrial Hygienist with the Occupational Safety and Health Administration, an agency of the DOL, from June 2016 until July 2023. In 2020 and 2021, Kang was a full-time employee of the DOL and earned over $85,000 annually.

In April 2020, Kang submitted a false PUA application to the Division of Unemployment Assistance (DUA). In the application, Kang claimed under the penalty of perjury that he was "self-employed, an independent contractor, or a gig worker and COVID-19 had severely limited his ability to perform his normal work," and that he had not earned more than $89 a week since March 8, 2020. The DUA approved Kang's claim, and through September 2021 Kang subsequently submitted weekly certifications to the DUA claiming that he did not work and did not receive any income during those weekly periods. Based upon his application and weekly certifications, Kang received $45,868 in PUA benefits to which he was not entitled. Kang was ordered to pay restitution in the amount of $45,868. (Source)

DEPARTMENT OF WAR / INTELLIGENCE COMMUNITY

Former Air Force Secretary Frank Kendall Has Security Clearance Revoked For Disclosing Classified Information About Air Force One - August 7, 2026

The U.S. Department of War has revoked former Air Force Secretary Frank Kendall's eligibility to access classified information over what the department says was an unauthorized disclosure involving Air Force One's capabilities. A Pentagon spokesperson announced the move saying it took effect immediately and also bars Kendall from holding any sensitive position.

"This action follows his unauthorized disclosure of classified information regarding Air Force One's capabilities to a media outlet. Safeguarding classified information is a non-negotiable duty. Those who violate that trust forfeit the privilege of access and any role requiring it."

The move comes days after The Wall Street Journal published a report comparing the capabilities of the Qatari-donated Boeing 747-8, now used as a presidential aircraft, with the older Air Force One jets. Kendall was among the former officials quoted in the report. (Source)

Defense Intelligence Agency Insider Threat Program Employee Pleads Guilty To Attempting To Provide Classified Information To Foreign Government - August 27, 2026

Nathan Vilas Laatsch, 29, is a former IT specialist for the Defense Intelligence Agency (DIA). Laatsch betrayed his oath by offering classified information to a foreign government, the very thing he was supposed to prevent as an employee of DIA's Insider Threat Program.

Laatsch became a civilian employee of the DIA in 2019, where he worked with the Insider Threat Division and held a Top Secret security clearance. In March 2025, the FBI learned that Laatsch offered to provide classified information to a friendly foreign government. Soon thereafter, Laatsch began communicating with an individual he thought was affiliated with that foreign government but was actually an FBI agent.

In late April 2025, Laatsch began transcribing classified information to a notepad at his desk and, over the course of approximately three days, repeatedly took the information from his workspace. After those three days, Laatsch deposited the classified information on a thumb drive at a public park in northern Virginia for the foreign government to retrieve. The FBI retrieved the drive, which contained multiple typed documents, each containing information up to the Secret or Top Secret level. It also contained a message from Laatsch, in which he indicated that he had chosen to include "a decent sample size" of classified information to "decently demonstrate the range of types of products" to which he had access.

After receiving confirmation that the drive had been received, Laatsch communicated that he was interested in "citizenship" to the foreign country. Laatsch also stated that, though he was "not opposed to other compensation," from a financial standpoint, he did not need "material compensation."

A week later, in mid-May 2025, the FBI agent advised Laatsch that the agent was prepared to receive additional classified information. Between May 15 and May 27, 2025, Laatsch again repeatedly transcribed multiple pages of notes while logged into his classified workstation and took the classified information away from his workstation hidden in his clothing.

On May 29, 2025, Laatsch arrived at a prearranged location in northern Virginia, where he again transmitted multiple classified documents. Laatsch was arrested upon the FBI's receipt of the documents. (Source)

Maryland National Guard Member Pleads Guilty To $2.2 Million+ Money Laundering Scheme - August 13, 2026

From May 22, 2019, through November 28, 2022, Alagborenepakake Opuiyo, 32,conspired to launder funds which were stolen through a variety of fraudulent means, including romance fraud and business email compromise schemes. Opuiyo and his co-conspirators, including some who resided in Maryland, opened bank accounts that served as drop accounts. These accounts were opened or controlled as part of the scheme to receive money from the fraud victims.

After receiving the funds in the drop accounts, Opuiyo and his co-conspirators transferred the money to other accounts that either they or their co-conspirators controlled. Additionally, Opuiyo and his co-conspirators directly withdrew money in cash. As a part of the scheme, romance-fraud victims believed they were communicating with individuals on online dating websites. The victims wired thousands of dollars to bank accounts that Opuiyo and his co-conspirators controlled.

Opuiyo and his co-conspirators used these bank accounts to initiate account transfers, such as withdrawing cash, obtaining cashier's checks, and writing checks to other individuals and entities to hide the true ownership and source of the assets. The loss resulting from these transactions was at least $2,270,668.40. This conspiracy laundered funds from at least 33 different victims. (Source)

Air Force Active Duty Member Settles False Claims Act For Submitting Fraudulent Application For PPP Loan For $16,000+ - August 3, 2026

In April 2021, Negleatta Davis prepared and submitted, or caused to be submitted, false and fraudulent documents and a false and fraudulent application to obtain a PPP loan totaling $14,375, in her name as sole proprietor.

The loan was forgiven and paid by the SBA, plus a lender fee of $2,500 and interest of $63.09, for a total of $16,938.09. Davis registered a business, Apple Jreamzz Treats & Things, with the State of Nevada while she was stationed there, on July 1, 2020. The United States contends that Davis fraudulently obtained the PPP loan at least in part because Apple Jreamzz Treats & Things was not established until July 2020, after CARES Act eligibility. (Source)

SECURITY CLEARANCE RELATED / WHISTLEBLOWERS

No Incidents To Report

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

FBI Supervisor Confesses To Stealing Nearly $1 Million In Crypto Belonging To Suspect FBI Was Investigating - August 6, 2026

An FBI supervisory agent is accused of stealing about $1 million in cryptocurrency from accounts belonging to a suspect overseas that the FBI was investigating.

According to court documents, FBI agent Patrick Steven Yaroch who served as a supervisor in the counterintelligence division. He came forward to confess, telling a Department of Justice (DOJ) employee that the theft was "eating him up inside," and he wanted to "get it off his chest."

Yaroch who had been with the FBI since 2017 became aware of the cryptocurrency accounts in November 2024 in the course of his investigative work. Prosecutors say Yaroch became frustrated that the FBI "could not or would not act" on the accounts and allegedly decided to transfer the funds himself.

Yaroch allegedly used his top-secret security clearance to gain access to the adversarial accounts, initiating 10 to 12 transfers into his own account amounting to around $1 million.

Investigators also found searches on Yaroch's phone asking ChatGPT how to invest or spend $1 million to maximize returns. According to court documents, he also told ChatGPT he was 37 with a young family and hoped to retire around age 40 in a country such as Portugal.

In a statement, the FBI said it took immediate action, firing Yaroch on July 31, the same day as his arrest. "The individual has since been fired from the Bureau. We hold our employees to the highest ethical standards, and this conduct is not tolerated at the FBI," a spokesperson told NBC News. "We are conducting a thorough investigation in the aftermath, and as this is an ongoing matter, we will have no further comment."

Yaroch was charged with interstate transportation and receipt of stolen goods, securities, and monies. (Source 1, Source 2)

Arrest Warrants Issued For Current & Former Metropolitan Police Department Members For $441,000+ Of Overtime Fraud - August 18, 2026

Arrest warrants were issued for current and former Metropolitan Police Department (MPD) members: Peter Sheldon, Frantz Fulcher, Thomas Krmenec, Bernadette Richardson, Dorrie Smith Cleere, and Johnnie Dyer. The warrants issued will lead to arrests on charges for fraudulently claiming overtime and for hours not worked during the calendar year 2024.

During the calendar year 2024, multiple MPD employees in the Fifth District submitted false claims for overtime hours or regular tour duty hours they did not work. The evidence shows these employees manipulated official records, forged supervisory approvals, and/or claimed compensation while engaged in secondary employment.

The investigation relied upon numerous independent data sources, including Body-Worn Camera footage, radio and GPS records, cell site location data, cellular toll records, license plate reader data, annual leave records, travel records, email records, network data, access logs, personnel files, and overtime documentation submitted through MPD's Timesheet Manager Application (TMA) system. Collectively, these records demonstrated repeated and deliberate falsification of overtime submissions, and in some instances regular time submissions. (Source)

United States Citizenship & Immigration Services Employee Charged With Stealing $60,000 From Labor Union / Used Funds For Personal Expenses - August 20, 2026

Carol Aguja, 55, was an Immigration Services Officer employed by the United States Citizenship and Immigration Services (USCIS).

Between approximately 2015 and August 2024, Aguja also served as Treasurer of the American Federation of Government Employees Local 38 (AFGE Local 38), a labor organization that represented USCIS employees who lived in Massachusetts, Rhode Island and New Hampshire.

Between 2019 and 2024, Aguja defrauded AFGE Local 38 by siphoning funds from the union bank account to pay for her own personal and non-union related expenses. As part of her fraud scheme, Aguja is also alleged to have paid union expenses out of her personal accounts and commingled union and personal funds to conceal her embezzlement. Specifically, Aguja is alleged to have used the AFGE Local 38 credit card to pay approximately $12,508 for personal expenses such as restaurant meals, bills, clothing and dance lessons. She is further alleged to have made 128 cash withdrawals totaling over $23,700 from the AFGE Local 38 account, and to have transferred over $25,000 from the AFGE Local 38 account to her personal accounts. (Source)

U.S. Customs Border & Protection Officer Sentenced To Prison For Accepting Multiple $10,000 Bribes To Allow Drugs To Enter The U.S. Through Their Inspection Lanes / Used Funds For Luxury Lifestyle - August 7, 2026

Customs and Border Protection (CBP) Officers Jesse Garcia was sentenced in federal court to 9 years in prison for allowing drug-laden vehicles to pass through his inspection lane at the Tecate Port of Entry in California on behalf of the Sinaloa Cartel.

The sentencing follows a long-term, multi-agency investigation that uncovered a significant corruption scheme involving Garcia and his co-defendant, then CBP Officer Diego Bonillo.

Both officers pleaded guilty in July 2025, with Garcia admitting that since at least 2021, he provided the Sinaloa Cartel-linked drug trafficking organization with his duty schedules and lane assignments so vehicles carrying cocaine, methamphetamine, and fentanyl could pass through his lanes unchecked. Bonillo was sentenced to 15 years in prison in November 2025.

In exchange for his assistance, the Garcia received at least $10,000 for each drug-filled vehicle he allowed to pass through the port. Evidence further showed that his illicit proceeds funded a lifestyle far beyond his government salary, including luxury purchases, a high-end vehicle, a San Diego residence, co-ownership of an equine racing business, and construction of a ranch in Mexico. (Source)

Miami Gardens Police Officer Pleads Guilty To $63,000 Of COVID-19 Relief Loan Fraud - August 17, 2026

Alvin Bernard, 38, was employed as a police officer with the Miami Gardens Police Department (MGPD) and also served as the sole manager and authorized representative of Vanity Properties LLC. Acting on behalf of the company, Bernard submitted an online EIDL application that falsely represented Vanity Properties' gross revenues in order to qualify for federal disaster assistance.

Bernard falsely certified that Vanity Properties generated $127,881 in gross revenues for the 12-month period preceding Jan. 31, 2020. In reality, the company had not earned those revenues. Based on the false information, the SBA approved and disbursed a $63,900 EIDL by electronic funds transfer into Vanity Properties' bank account. (Source)

6 Police Department Employees Placed On Administrative Leave For Misusing Flock Camera Systems Website - August 3, 2026

Savannah Police Department discovered that six employees (four officers and two civilians) misused the department's Flock camera system through unauthorized searches unrelated to law enforcement, including lookups on personal acquaintances and family members, with one officer also granting unauthorized access to an outside agency. The misuse was detected by an automatic audit-assist tool that flagged 127 of approximately 39,000 searches in 2026, with manual review identifying 34 searches deemed unjustified by these six staff members. All six employees were placed on administrative leave following the findings. The department committed to implementing formal usage policies and conducting weekly audits to prevent future misuse." (Source)

2 Bureau of Prisons Correctional Officers Sentenced To Prison For Accepting $150,000+ In Bribers To Smuggle Contraband Into Prison - August 21,2026

Robert Cochran and Tejuana Dillard will go from being federal prison guards to federal prison inmates after each was sentenced to 30 months' incarceration in separate cases after getting caught smuggling contraband into the Forrest City Federal Correctional Complex (FCC) in Arkansas.

An investigation revealed that while Cochran was employed as a correctional officer at Forrest City FCC, he received approximately $58,775 from friends and family of the inmates at the prison to bring contraband, including rolling papers, tobacco, Gucci sunglasses, and over the counter drugs, into the facility. Cochran was captured on video footage in February 2023 leaving bags containing contraband in an office while on duty. After Cochran left the office, an inmate would enter to retrieve the items. Cochran later admitted he was paid to bring items into the prison for inmates.

Through a separate investigation, it was determined that Dillard, who was employed for 13 years as a correctional officer between 2008 and July 2021 at Forrest City FCC, smuggled contraband cigarettes into the prison throughout 2020. Dillard received in total $91,788 to provide the cigarettes to two inmates, who later sold the contraband cigarettes to other inmates in the facility. Dillard, in an interview with federal agents, admitted to smuggling cigarettes while she was employed as a correctional officer, but stated she had only done so "a couple of times." At the time of her interview with the federal agents, Dillard knew the statements she made were false. (Source)

Federal Correctional Officer Pleads Guilty To Distributing Methamphetamine To Inmate For $15,000 Bribe Payment - August 6, 2026

Antonio Ray Ramirez, 35, pleaded guilty to one count of distributing methamphetamine.
in August 2024, while working as a Correctional Officer, Ramirez knowingly distributed 869 grams of methamphetamine and 127 grams of heroin in the Federal Correctional Institution in Herlong, California.

When beginning an overnight shift, Ramirez smuggled the drugs into the prison by evading security screening, hid them in a laundry room, and told an inmate where to find them. Ramirez received $15,000 in payment for smuggling the drugs. The drugs were eventually recovered from the inmate by other correctional officers. (Source)

Federal Corrections Officer & Wife Plead Guilty To Accepting $6,650 In Bribes To Smuggling Contraband & Drugs Into Prison - August 5, 2026

A correctional officer (Paul Betancourt, 38) at a federal prison in Santa Barbara County (CA) and his wife (Sylvia Betancourt, 49) pleaded guilty today to smuggling contraband including a drug used to treat opioid addiction to a prison inmate in exchange for a total of $6,650 over several months.

Paul Betancourt was employed by the Federal Bureau of Prisons (BOP) as a correctional officer at Federal Correction Complex (FCC), Lompoc. From May 2023 to September 2023, Paul Betancourt agreed to provide contraband to an FCC Lompoc inmate. Sylvia Betancourt received payment and contraband from the inmate through the inmate's intermediaries, which she then delivered to her husband.

The defendants admitted that on at least 13 occasions, they met with, or received payment from, a Lompoc inmate or one of the inmate's intermediaries for the delivery of contraband, including controlled substances such as suboxone. The payments ranged from $100 to as much as $1,500, according to court documents. In total, the inmate paid the defendants $6,650 to provide contraband to him at FCC Lompoc. (Source)

Federal Bureau Of Prisons Correctional Officer Charged With Accepting $60,000 In Bribes To Smuggle Contraband / Drugs Into Prison - August 12, 2026

Joseph Templeton, 30, while employed as a correctional officer at the Bennettsville Federal Correctional Institution in South Carolina, accepted more than $60,000 in bribes from a prison inmate and others associated with the inmate. In exchange for those bribes, Templeton smuggled contraband into the prison, including cell phones, cell phone accessories, cigarettes, and THC. Templeton falsely processed the contraband as a contraband seizure before distributing the contraband within the prison. (Source)

LAW FIRMS

Law Firm Paralegal Guilty Of Embezzling $1.8 Million+ Over 6 Years / Used Funds To Purchase 2 Homes - July 31, 2026

From 2010 to 2018 Bobbie Ellis worked for a small law firm in Mandeville, Louisiana. Ellis performed duties of an office manager, bookkeeper, and paralegal. In those roles, Ellis had access to the law firm's financial records, bank accounts, notary stamp, and other legal documents.

From at least 2012 to 2018, Ellis, without authorization, accessed bank accounts controlled by the law firm and forged her employer's signature on numerous checks stealing over $1.8 million.

Ellis used the fraudulently obtained proceeds to purchase a home in Georgia and another home in Florida. Ellis also fraudulently used a credit card linked to her employer.

Ellis charged over $945,000 in unauthorized purchases, including expenses related to vacations, hotel stays, retail store purchases, restaurants, and purchases for her children and pets. To conceal her fraud, Ellis used funds from bank accounts controlled by the law firm to pay for her fraudulent credit card charges. In total, Ellis embezzled $1,861,575.75 from bank accounts controlled by her employer. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

New Mexico State Representative & Business Owner Convicted For $5 Million Fraud Scheme - August 14, 2026

A federal jury convicted former State Representative Sheryl Stapleton, 69, and her friend Joseph Johnson, 75, on all counts with which they were charged stemming from a yearslong scheme in which Stapleton used her position at Albuquerque Public Schools (APS) New Mexico and in the legislature to steer millions of dollars in funding to Johnson's company and secretly received approximately $1.15 million from the company.

From about July 1, 2013, through June 30, 2021, Stapleton used her position at APS as Director of the Perkins Project and Career and Technical Education (CTE) Coordinator to direct approximately 40% of APS's non-personnel CTE funding to Robotics Management Learning Systems (Robotics), a Washington, D.C., company owned and operated by Johnson, for use of and support for the CyberQuest software in APS classrooms.

From 2013 through 2021, APS paid Robotics approximately $3.25 million under contracts for the software and related services, including approximately $2.52 million in federal Perkins funds.

During that time, Stapleton served as a New Mexico state representative for District 19 from1995 through 2021 and was majority floor leader from 2017 through 2021. While serving in the Legislature, she sponsored and advocated for legislation and capital outlays that directed additional funding to APS for CTE programs. She then used her position at APS to direct CTE funding to Robotics and facilitate contracts for the company through procurement exemptions, sole-source contracts and, later, a request for proposals. (Source)

Stapleton Used Approximately $1,152,506 Of Robotics Funds For:

$286,772 to S. Williams & Associates, a company she owned and controlled;
$313,123 to Taste of the Caribbean, an Albuquerque restaurant she owned and her family members operated;
$479,961 to Ujima Foundation, a nonprofit entity Stapleton and Johnson operated together; and
$72,649 to other parties for goods and services benefiting Stapleton, including remodeling work on her home.

2 South Dakota Housing Authority Employees Plead Guilty To Embezzling $3.5 Million Of Federal Funds Over 6 Years - August 6, 2026

Eric Shepherd, 53, was the executive director of the Sisseton Wahpeton Housing Authority (SWHA) between September 2019 and July 2025. Olivia Locke, 60, was the chief financial officer. During that time, Locke and Shepherd issued and cashed over $3,500,000 in unauthorized SWHA checks for their personal enrichment. (Source)

City of Fresno California Art Council Manager Sentenced To Prison For Embezzling $1.8 Million+ Of Public Funds / Used Funds For Gambling, Vacations Etc. - August 10, 2026

Suliana Caldwell worked as the Fresno Art Council's operation's manager from 2021 to February 2026. In this position, she managed the Fresno Arts Council's bank accounts, payroll, grants, donations, and general finances. Her duties also included providing periodic financial updates and reports to the executive director, board members, and the City and County of Fresno.

Beginning in 2022, Caldwell embezzled funds by making unauthorized withdrawals of money from the FAC's bank accounts.

In 2023, after the Fresno City Council designated the FAC to administer its Measure P grant money, Caldwell significantly increased the amount of money she stole from the FAC's accounts and ultimately took more than $80,000 per month on average. Measure P is a tax initiative approved by Fresno voters in 2018 to provide funding for parks, trails, and the arts, among other things.

Caldwell concealed her theft by using her position of trust as the operations manager to falsify financial reports, which omitted her theft and represented that there were significantly higher balances in the FAC's bank accounts than was true. She then presented the false reports to the FAC's executive director, board members, and others to trick them into believing everything was okay. Caldwell received an enhancement to her sentence because of this abuse of trust.

In total, Caldwell stole over $1.8 million from the FAC. She then used the money to gamble at local casinos where she enjoyed various VIP statuses, pay for vacations, and for other improper personal expenses. The FAC detected Caldwell's theft in February 2026 when one of its checks bounced. Caldwell was subsequently fired and charged in this case. (Source)

Massachusetts Mayor Charged With Fraudulently Obtaining $1.5 Million+ Of COVID Loans / Used Funds For Campaigning - August 26, 2026

The Mayor of Lawrence, Massachusetts (Brian DePena, 61) has been indicted by a federal grand jury in Boston. The charges state the Mayor with allegedly obtaining over $1.5 million in COVID small-business loans. It is alleged that the money was used to fund his campaign account, pay personal taxes and pay more than $880,000 in high-interest, hard-money mortgages on properties he owned in Lawrence. (Source)

Massachusetts State Representative Charged With Fraudulently Obtaining $700,000+ Of COVID Loans / Used Funds To Buy Real Estate & Loan Money - August 26, 2026

The Massachusetts State Representative for the 16th Essex District (Francisco Paulino, 46) representing Lawrence and Methuen, was arrested and charged with fraudulently obtaining over $700,000 in COVID unemployment insurance benefits and small-business loans, and using the proceeds to buy real estate and loan money to clients of his mortgage business, before he was elected to public office. (Source)

City Commissioner Sentenced To Prison For Fraudulently Obtaining Nearly $950,000 In Covid PPP Loans – August 14, 2026

A former City of Sweetwater (FL) commissioner, Sophia Lacayo, 48 was sentenced to 18 months in federal prison for fraudulently obtaining nearly $950,000 in Paycheck Protection Program (PPP) loans by submitting falsified payroll records, fabricated tax documents, and other fraudulent submissions to lenders administering pandemic-relief funds.

Lacayo owned Lacayo Trade Group Inc. (Lacayo Trade) and exercised significant control over QC Tax Pro Systems LLC (QC Tax) and QC Trade Group LLC (QC Trade). Lacayo submitted, and caused to be submitted, fraudulent PPP loan applications on behalf of the three companies in order to obtain pandemic-relief funds to which the companies were not entitled.

Lacayo and her companies fraudulently obtained approximately $948,325 in PPP loan proceeds, including two $251,465 loans obtained on behalf of QC Tax, a $117,500 loan obtained for QC Trade, and a $327,895 loan obtained for Lacayo Trade. (Source)

Michigan Township Treasurer Pleads Guilty To Stealing $647,000+ Over 11 Years / Used Funds To Build Vacation Home, Etc. - August 6, 2026

Marilyn Harp, 74, admitted that she took Township funds and used them for herself, which included building a vacation home, taking vacations and purchasing luxury items. Harp served as the treasurer of Ionia Township between 1984 and 2025. Her position put her in charge of collecting property taxes from residents of Ionia Township, which she was supposed to deposit into Township bank accounts and be used for public services.
The criminal charge alleges that Harp committed fraud between 2014 and 2025 when she diverted much of this money-- $747,025-- for her own benefit.

When others began to suspect that Harp was stealing public funds, she attempted to cover her tracks by fabricating some records and destroying others. As part of her plea agreement, Harp agreed to forfeit $647,698 that federal investigators connected to the fraud scheme and seized during the investigation. (Source)

Contractor Employee For Maryland State Department Of Labor Contractor Pleads Guilty To Embezzling $550,000 - August 10, 2026

Beginning in January 2021, and continuing until December 2021, Katrina McCant, 41, used her position as a contractor for Company #1 to enriched herself by fraudulently obtaining unemployment insurance (UI) benefits while working for the MD-DOL.

McCant used her insider access to MD-DOL data and databases to upload and approve documents submitted in support of UI claims. Some of the claims she initiated herself while others she took over by changing the claimant's email address and name to her own.

In furthering the scheme, she removed holds on UI claims, certified weeks, and engaged in other actions to facilitate fraudulent UI benefit payments. As part of the scheme, McCant changed the names of the claimants to facilitate the direct deposit of funds into her financial accounts. She also used the personal identifiable information (PII) of multiple real people, who were aggravated identity theft victims, to make changes to UI claims in the MD-DOL system. McCant agreed to pay restitution to the MD-DOL of at least $550,000. (Source)

County Employee Pleads Guilty To Embezzling $431,000+ From Tax Assessor-Collector's Office - August 11, 2026

Gina Upshaw, 65, was a bookkeeper for the Cherokee County Tax Assessor-Collector's Office in Texas from 2008 through January 2022.

The Tax Assessor-Collector's Office collects both property taxes and motor vehicle sales taxes, as well as registration fees, from Cherokee County residents, for both Cherokee County and the State of Texas. The office receives these payments in the form of both cash and checks.

During her employment as a bookkeeper for the office, Upshaw was responsible for making daily deposits of the cash payments at a local bank. Instead of doing so, Upshaw stole cash payments totaling $431,375.91. (Source)

Rhode Island Department of Human Services Supervisor Pleads Guilty To $300,000+ Fraud Scheme For Supplemental Nutrition Assistance Program / Used Funds For Personal Purchases - August 5, 2026

A Providence Rhode Island Department of Human Services (RI-DHS) supervisor has pleaded guilty in federal court to charges stemming from her misuse of her official position to improperly access and exploit the personal information and benefits of Supplemental Nutrition Assistance Program (SNAP) recipients.

Nadine Jean Baptiste, 59, admitted to repeatedly accessing SNAP Electronic Benefit Transfer (EBT) card information, conducting unauthorized telephonic balance inquiries, and altering PIN numbers associated with those cards. Many of the affected individuals were juveniles, homeless, or incarcerated at the time their information was accessed.

In total, EBT cards containing more than $300,000 in SNAP benefits were improperly accessed. It is further alleged that Jean Baptiste and her daughter used fraudulently accessed SNAP benefits to make personal purchases.

The investigation began in September 2023 after the Rhode Island Office of Internal Audit received multiple complaints from SNAP recipients through its Fraud Hotline, reporting that they never received the EBT cards issued to them. (Source)

County Employee Charged For Embezzling $55,000+ Of Federal Grant Funding - August 10, 2026
Justin Roper is the former Chief of the Washoe County Department of Alternative Sentencing.

The Department of Alternative Sentencing received approximately $1.3 million in grant funding from the Bureau of Justice Assistance, a component of the Justice Department. As alleged, from November 2024 to December 2024, Roper embezzled $55,593.52 of federal grant funds. (Source)

3rd Georgia State Representative Pleads Guilty To $17,000+ Of Pandemic Unemployment Fraud / 2 Others Convicted - July 30, 2026
Sharon Henderson, a suspended member of the Georgia House of Representatives, pled guilty in federal court to making false statements to fraudulently obtain thousands of dollars of emergency pandemic-era unemployment assistance payments.

Henderson fraudulently collected $17,811 of pandemic unemployment benefits as a result of the false statements in her application and weekly certifications.

2 other Georgia State Representatives were previously convicted of similar pandemic unemployment assistance fraud:
Karen L. Bennett, former State Representative pled guilty on January 21, 2026, to federal charges of making false statements to collect $13,940 of pandemic unemployment benefits.
Dexter L. Sharper, former State Representative pled guilty on March 11, 2026, to federal charges of making false statements to collect $13,825 of pandemic unemployment benefits. (Source)

City Clerk Pleads Guilty To Stealing $5,000+ By Making Unauthorized Charges On City Credit Card For Dining, Designer Clothing, Etc. - July 31, 2026
The FBI met with City of Edison Georgia representatives on Dec. 7, 2023. During the meeting, one individual explained to investigators he had been contacted by Tami Fincher, the City's former Clerk, earlier in the year and advised that Edison was unable to pay a loan they owed. City representatives began to investigate the issue and immediately recognized significant financial mismanagement of the city's accounts. Edison received more than $10,000 in federal program funds annually.

Fincher began working as the City Clerk for Edison in March 2018 and was responsible for the City's finances. Fincher was issued a city credit card. A review of Fincher's city credit card statements revealed a large quantity of inappropriate personal charges made using that card, including dining out, dog treats, Amazon purchases, and designer clothing. Between 2018 and 2023, Fincher made more than $5,000 in unauthorized personal purchases using that card. Fincher resigned from her position in July 2023. (Source)

Omaha City Employee Sentenced To Prison For Sex Trafficking - August 21, 2026
Amy Hicks was sentenced to 15 to 30 years in prison for income tax evasion, felony pandering, and criminal conspiracy.

Between 2022 and 2024, Hicks contacted dozens of people on commercial sex apps and recruited them, including an 18-year-old victim, and claimed she made tens of thousands on this. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Principal & 2 Others Sentenced To Prison For $ 1 Million+ Procurement Fraud Scheme Over 10 Years - August 20, 2026
A former Chicago school principal and 2 others have been sentenced to federal prison for their roles in procurement fraud schemes that defrauded a pair of school systems and a non-profit organization out of more than $1 million.

Brian Metcalf, Kimberly Maddox, and James Campbell schemed to illegally profit from various roles Metcalf held in school systems in Chicago and Indianapolis, as well as a non-profit corporation. Over the course of nearly ten years, Metcalf and Maddox falsely claimed that Maddox or her spouse were providing services to the schools and the non-profit corporation, when in reality, no such services were provided.

As a result of Metcalf's and Maddox's fraud, the school systems and the non-profit organization paid Maddox nearly $700,000, which she split with Metcalf.

While Metcalf and Maddox were engaging in their fraud, Campbell, who worked as a consultant, approached Metcalf and said he wanted to join the scheme. At that time Metcalf was serving as the superintendent of a school system in Indianapolis. Metcalf caused the Indianapolis school system to pay Campbell nearly $400,000 based on bogus invoices for consulting work that was never performed. Campbell split those fraud proceeds with Metcalf. (Source)

School District Employee Sentenced To Prison For Embezzling $261,000+ / Used Funds To Pay Personal Credit Cards - August 14, 2026
Danielle Mittermeyer, 47, previously worked as the business official for the School District of Alma Center-Humbird-Merrillan in Wisconsin. She was responsible for making payments for the district, collecting and depositing cash, and tracking finances.

Between 2021 and 2025, she embezzled more than a quarter million dollars through a variety of means, including skimming cash and using district funds to pay the balance on her personal credit card. She concealed her criminal conduct from the district and its auditors by duplicating invoices from legitimate vendors, altering check reports presented to the school board, setting herself and her credit card company up as vendors in the district's accounting software, and keeping a second (fraudulent) cash receipt book. Mittermeyer was ordered to pay $261,690 in restitution. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Union Financial Secretary Sentenced To Prison For Stealing $54,000+ Over 9 Years - August 4, 2025

For nearly 9 years, David Scofield, 65, used his position as the financial secretary for Brotherhood of Railroad Signalmen, Local Lodge 21, in Missouri to steal more than $54,000 from the union. He issued unauthorized checks, made personal payments from the union account, and conducted hundreds of online transactions for his own benefit. He then hid his fraud by falsifying records. (Source)

BANKING / FINANCIAL INSTITUTIONS

Credit Union Branch Manager Sentenced To Federal Prison For Stealing $381,000 From Elderly & Incapacitated Customers / Used Funds For Gambling, Etc. - August 12, 206

From 2014 through December 2022, Teresa Palmer worked as the branch manager of a credit union in Columbus, Indiana. In her role, Palmer had access to customer accounts and was authorized to withdraw funds or issue cashier's checks when a customer approved a transaction.

In 2022, the credit union terminated Palmer after discovering she had forged customer signatures on banking documents. Shortly after her termination, a client notified the credit union of unauthorized transactions in her father's account. An internal investigation confirmed that Palmer had not only forged signatures but also withdrawn funds from the client's account without permission. Further review revealed additional victims: Palmer had stolen from four customer accounts over a two-year period.

Investigators determined that between January 2021 and December 2022, Palmer targeted accounts belonging to elderly customers or individuals unable to regularly monitor their finances.

Using her work computer and banking software, Palmer executed unauthorized cash withdrawals and diverted the funds for personal expenses, including gambling. Palmer also fraudulently issued cashier's checks from customer accounts, making them payable to third parties.

She forged the payee's endorsement, printed the checks, and stamped "for deposit only" or forged a customer's signature before presenting the checks to a teller, falsely claiming customer approval. Once the checks were converted into cash, Palmer kept the money for herself.
In total, Palmer conducted hundreds of unauthorized transactions, stealing $381,400.05 from several elderly victims, including one individual with dementia. (Source)

Credit Union Manager Pleaded Guilty To Stealing $185,000 - July 31, 2026

On February 4, 2026, Alexa Braud, entered a credit union located in Gretna, Louisiana where she was a bank manager, and took $185,000 in United States currency. The deposits of the credit union are insured by the National Credit Union Administration. (Source)

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

Operations Manager Of Wholesale Drug Distributor Sentenced To Prison For Role In Illegal Scheme To Buy $47 Million+ In Prescription Medications & Resell For Profit - August 4, 2026

For several years, Frank Incognito, 46, worked as an operations manager of a wholesale drug distributor, operating under the New Jersey corporations of VRC Medical Services and Investigational Drug Delivery (VRC/IDD).

Incognito conspired with others at VRC/IDD, as well as multiple doctors, to obtain expensive prescription medications that Incognito and his coconspirators otherwise would not be able to obtain on their own.

These medications were "straw-purchased" through the doctors' medical practices, and then Incognito and his co-conspirators illegally transferred and resold those medications.

Primarily, these medications were cold-chain biologic infusion medications that typically are used to treat cancers, macular degeneration, and autoimmune diseases.

In purchasing the drugs, Incognito and his coconspirators made numerous false and misleading representations to the pharmaceutical manufacturers and authorized distributors, including that the doctors were purchasing the drugs to treat their own patients, and that the drugs would not be resold or redistributed to others.

In actuality, none of the drugs were administered to any of the doctors' own patients but were ultimately sold to customers of the VRC/IDD businesses for a profit.

The scheme in which Incognito participated ran from approximately June 2012 through January 2019. During this time, Incognito conspired with others to buy and sell more than $47.7 million worth of the prescription drugs. Incognito is the third defendant who has been sentenced in connection with this fraudulent scheme, in addition to doctors Anise Kachadourian and Joel Lerner. (Source)

Employee For Medical Clinics Sentenced To Prison For Embezzling $539,000+ / Used Fund To Pay For New Cars, Time Share, Credit Cards - August 4, 2026

Brooke Duck, 31, was employed by two medical clinics with offices in Lafayette and Baton Rouge, Louisiana, He and had access to the clinics' credit cards and bank accounts. Between May 2020 and October 2023, Duck used the clinics' credit cards for unauthorized personal purchases, including a $15,000 payment for a time-share vacation property.

She then used funds drawn from the clinics' bank accounts to pay for new cars, fancy consumer products, pay credit card balances associated with those purchases. In total, Duck caused $539,451.41 in unauthorized credit card transactions for her personal use and financial gain. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION / EMPLOYEES WHO LEAK INFORMATION TO THE PUBLIC

Weekly EchoMark Listing Of Employee Data Leaks

Philips Medical Systems Engineer Convicted For Stealing Trade Secrets On Behalf Of Chinese Competitor - August 24, 2025

CHIH-YEE JEN worked as an engineer at Philips' facility in Aurora, Ill., where employees researched, developed, and manufactured X-ray tubes used in computed tomography (CT) medical imaging machines.

Through its Dunlee brand, Philips spent years developing proprietary X-ray technology and selling various devices to medical facilities. In 2017, as Philips prepared to close the facility in Aurora, China-based KUNSHAN GUOLI ELECTRONIC TECHNOLOGY CO. LTD. and a Kunshan GuoLi vice president, XIAOQIN DU, began communicating with Jen about creating a U.S. subsidiary for Kunshan GuoLi to help it compete with Philips in developing, manufacturing, and selling X-ray tubes.

While still employed at Philips, Jen began sharing confidential Philips documents with Kunshan GuoLi and Du and successfully recruited multiple Philips engineers to join him at the Kunshan GuoLi subsidiary. Jen copied Philips' proprietary X-ray trade secret information from internal Philips databases and used the stolen information in connection with his new work developing the technology for the Kunshan GuoLi subsidiary. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

3M Expert Witness Used ChatGPT To Create 90% Of Content Used To Testify In Lawsuit Involving 3M - August 20, 2026

An expert witness (Josh Autenrieth) was hired by 3M to testify in a bombshell lawsuit against 3M over a Houston explosion that killed three people.

3M hired Autenrieth as an expert at $475 an hour to prepare a report about the explosion – which turned out to be up to 90% composed by ChatGPT. 3M paid Knighthawk Engineering about $90,000 for Autenrieth's report, according to court transcripts.

The unveiled chatbot prompts, detailed by news outlet 404 Media, show Josh Autenrieth, an expert with Knighthawk Engineering, telling ChatGPT to help him "create an exceptional expert witness report defending the standard of care at 3M" and to "show how 3M is 0% at fault for the explosion at Watson Grinding."

Knighthawk's Vice President Nathan Knight ripped the report as "fake news" and said the company "stands behind the professionalism and integrity of its engineers.

Will Moye, one of the plaintiffs' attorneys, found during discovery a five-page document that appeared to be AI generated. Moye demanded that 3M's legal team offer up the prompts Autenrieth had used – which resulted in 350 pages of ChatGPT conversations.

The ongoing litigation is one of several high-profile cases over who is responsible for a 2020 blast at Watson Grinding, a Houston manufacturing facility that leveled roughly 200 homes. Dozens of homeowners allege 3M failed to properly service the facility's gas detection system that caused the explosion. (Source)

Note:

This above incidents shows that prompts provided to a AI systems can be used as evidence during an investigation or court hearing.
Are your employees posting sensitive information into a AI system, that they shouldn't?
Do you have auditing capabilities to record what employee are directing AI systems to do?
How long are employee prompt records kept?

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

New FBI Alert To U.S. Companies Regarding DPRK North Korean Fraudulent IT Workers Hiring Scheme – July 31, 2026

North Korea relies upon a network of skilled Information Technology (IT) workers, deployed within and outside of North Korea, to obtain false identities and remotely earn income to fund North Korea's unlawful nuclear weapons and ballistic missile programs.

North Korean IT workers impersonate nationals of other countries to obtain work and income through online platforms operated by private companies for employment, procurement, and contracting of services. These workers seek out contracts with the intent of remitting their salaries to their parent North Korean agencies. They also pose an insider threat to companies and are involved in data exfiltration, cryptocurrency theft, and theft of sensitive information. North Korean IT workers employ increasingly sophisticated methods, including the integration of AI, to obfuscate their identities and expand their activities globally

Operatives have expanded targeting beyond large tech enterprises to mid-sized businesses, finance, healthcare, and public sector contractors while utilizing advanced location-masking tools

The U.S. Department of Justice and the FBI continue to prosecute domestic facilitators who host "laptop farms" with U.S. IP addresses, or supply stolen American identities to overseas operatives. (Source 1) (Source 2)

FBI Investigating North Korean Remote IT Staffer Working For U.S. Agency - August 10, 2026

The FBI is investigating how an unidentified federal agency was recently swept up in a yearslong campaign involving North Korean (DPRK) remote IT workers fraudulently obtaining jobs at major companies and other organizations. The North Korean campaign has been notorious for using remote IT contract jobs to infiltrate both Fortune 500 companies and smaller private sector firms.

During a panel discussion at a July 28, 2026 conference hosted by the Digital Government Institute in Washington, D.C., Todd Hemmen, deputy assistant director of the FBI's Cyber Capabilities Branch, was asked whether the DPRK remote IT worker issue had impacted government.

"Without getting into ongoing investigations, we identified just this past week a DPRK remote IT worker that was working for the federal government," Hemmen said. "Still kind of unpacking that recent case. It's actually a little bit baffling to me, not understanding this particular agency's process. But the short answer is yes, we are seeing remote IT workers not just in the private sector – although a vastly higher proportion in the private sector – but we're also seeing this impact the government to a degree."

The FBI declined to comment further on the story. It's unclear what agency was impacted, how long the intrusion lasted, and whether any sensitive data was stolen. (Source)

This above case is not the only case of DPRK infiltrating the U.S. Government. See next page.

Man Sentenced To Prison For Fraudulent Scheme That Assisted Foreign IT Workers (Posing As U.S. Citizens) With Obtaining Remote IT Positions With U.S. Companies - December 4, 2025

Minh Vong conspired with others, including William James, a foreign national living in Shenyang, China, to defraud U.S. companies into hiring Vong as a remote software developer. After securing these jobs through materially false statements about his education, training, and experience, Vong allowed James and others to use his computer access credentials to perform the remote software development work and receive payment for that work.

James submitted a fraudulent resume in Vong's name to a Virginia-based technology company for a web application developer position that required U.S. citizenship as a condition of employment. The resume falsely represented that Vong possessed a Bachelor of Science degree and 16 years of experience as a software developer. In fact, Vong did not have a college degree or experience in software development.

On March 28, 2023, Vong participated in an online job interview with the CEO of a Virginia-based company. Vong verified his identity and citizenship by showing his Maryland driver's license and U.S. Passport. Following the interview, the Virginia-based company hired Vong and assigned him to work on a contract for the Federal Aviation Administration (FAA) involving a particular software application used by various U.S. government agencies to manage sensitive information regarding national defense matters. The Virginia-based company provided Vong with a laptop to use in connection with his employment and the FAA authorized Vong to receive a Personal Identity Verification card to access government facilities and systems. Vong installed remote access software on the laptop to facilitate Doe's access to it and conceal his location in China.

Between March 2023 and July 2023, Doe used Vong's credentials to perform the software development work from his location in China. The Virginia-based company paid Vong more than $28,000 in wages for work he performed, portions of which Vong then sent overseas to Doe and other conspirators.

Vong admitted that the Virginia-based company was not the only company he and his co-conspirators defrauded. Between 2021 and 2024, Vong used fraudulent misrepresentations to obtain employment with at least 13 different U.S. companies, who collectively paid Vong more than $970,000 in salary for software development services that were, unbeknownst to them, performed by James or other overseas conspirators. (Source)

LARGE FINES OR PENALTIES THAT HAVE TO BE PAID BECAUSE OF INSIDER THREAT INCIDENTS

No Incidents To Report

INSIDER TRADING / STOCK TRADING & SECURITIES FRAUD

Senior Company Executive Charged With Insider Trading That Made Him $1.8 Million In Profit - August 20, 2026

Jesus Morell made over $1.8 million trading while in possession of material, non-public information he received through his employment. Morell was the President of two significant subsidiaries of HEICO and a member of the Board of Directors for a third subsidiary.

HEICO maintained policies prohibiting employees from trading in HEICO stock while in possession of material nonpublic information, which policies Morell acknowledged he understood on an annual basis.

On two separate occasions in 2022 and 2025, Morell purchased Class A common stock of HEICO in advance of the public quarterly earnings release but after receiving material non-public information concerning HEICO's actual or forecasted earnings for the quarter. Following the public release of HEICO's quarterly earnings information—which included financial data that was the same or very similar to the data Morell received before purchasing HEICO stock the price of HEICO's Class A shares rose and Morell quickly sold all of the shares he had purchased for a significant profit. In total, MMorell made more than $1.8 million in illicit profits by trading HEICO stock based on material, nonpublic information he misappropriated from his employer. (Source)

Company Finance Director Charged With Insider Trading That Made Him $338,000+ - August 20, 2026

Jesse Mitchell traded on misappropriated material nonpublic information ahead of public earnings announcements by his then-employer, and as a result, generated more than $338,000 in profits for him.

Around June 2024, Mitchell began working at TTD, a publicly-traded multinational technology company, as a Senior Director in TTD's financial planning and analysis team. In that role, Mitchell had access to TTD's confidential financial information and results, including revenue and earnings results and other financial metrics, before they were publicly disclosed. (Source)

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

Williams-Sonoma Executive Pleads Guilty To $16 Million Kickback, Fraud & Money Laundering Scheme - August 11, 2026

Eric Marsiglia, 52, admitted that from approximately 2018 through 2022, he conspired to defraud Williams-Sonoma, Inc. (WSI). During that time, Marsiglia served as WSI's Vice President of Engineering, Projects, Planning, Facilities, and Real Estate, with authority to enter vendor contracts. Marsiglia oversaw the selection and leasing of warehouse space throughout the United States as well as the purchase of steel racking, forklifts, and related warehouse logistics services.

Starting in 2018, Marsiglia accepted kickbacks from co-conspirators in exchange for steering WSI business to three New Jersey companies that supplied forklifts, racking systems, and machinery for warehouses.

Marsiglia set up a shell company, REM Group, to receive and conceal the kickbacks. In total, Marsiglia received over $12.2 million in warehouse kickbacks, which he concealed from WSI.

From 2020 through 2022, Marsiglia also conspired to divert real estate broker commissions associated with WSI warehouses. Marsiglia directed these payments to accounts held by REM Group.

He then distributed portions of those proceeds to himself and co-conspirators. Marsiglia concealed from WSI that he was causing broker commission payments to be diverted to accounts he controlled, rather than to the firm that was entitled to receive them. This scheme resulted in the misappropriation of over $4.1 million in broker commissions. (Source)

Non-Profit Chief Financial Officer Sentenced To Prison For Embezzling $2.1 Million+ - August 28, 2026
Jeffrey Keehn, 55, is the former CFO of the Child and Family Guidance Center in Imperial Beach, California

Keehn pleaded guilty to wire fraud after admitting he stole $2,109,786.56 from the non-profit over a period of approximately seven years. Keehn was ordered to pay full restitution in the amount of $2,109,786.56.

Keehn abused his position as CFO by secretly accessing the charity's checkbook, forging signatures and depositing fraudulent checks into his personal accounts. He also falsified QuickBooks entries and misrepresented the charity's available cash to conceal the scheme. As part of the investigation and forfeiture proceedings, the government successfully seized approximately $800,000 in assets, including multiple bank accounts, precious metals, a vehicle and his interest in a condominium in Oceanside, California. (Source)

Nike Employee Charged For Role In Running $1 Million Kickback Scheme Against Company - July 27, 2026
A former Nike music executive is facing a lengthy list of felony charges after prosecutors accused him of orchestrating a kickback scheme that siphoned more than $1 million from the sneaker giant through inflated payments to a music licensing firm run by a close associate.

Prosecutors allege that John Griffith, who worked as a music supervisor at Nike, funneled company funds toward a consulting firm operated by his friend Brad Mosher, paying fees far above what the services were actually worth.

Roughly half of those payments, prosecutors claim, were then routed back to Griffith through a shell company he controlled, effectively allowing him to pocket a cut of the inflated fees while Nike absorbed the cost.

Nike spends billions annually on advertising and regularly relies on well-known songs to anchor its marketing campaigns. Music supervisors are responsible not just for selecting which songs appear in commercials, films, and television projects, but also for navigating the often complicated legal process of clearing those songs for use, a responsibility that gives them considerable authority over vendor relationships and payments.

State prosecutors believe Griffith exploited that authority by directing Nike's money toward Mosher's firm, Good Measure LLC, a company that describes itself on LinkedIn as providing clearance and licensing services for music used in advertising.

After Nike paid Good Measure for its work, a portion of those funds was allegedly redirected to Quiver and Bow LLC, an entity tied to Griffith. Investigators say the scheme continued for roughly two and a half years, running from June 2020 through December 2022 before it was uncovered. (Source)

Executive Director In Goldman Sachs Investment Banking Division Convicted For Paying $1 Million+ In Bribes To Ghanaian Government Officials - August 6, 2026
Asante Berko, 52, conspired to pay more than $1 million in bribes to multiple Ghanaian government officials in connection with the development and financing of a power plant estimated to generate hundreds of millions of dollars in revenue.

Beginning in December 2014, Berko, a former Executive Director in the Investment Banking Division at Goldman Sachs, was responsible for securing and managing a deal between Aksa Enerji, a Turkish energy company and client of Goldman Sachs, and the Republic of Ghana, for the construction and financing of a power plant in Ghana amidst a national energy crisis in the country.

During the scheme, Berko and his co-conspirators paid and conspired to pay bribes to individuals at numerous levels of the Ghanaian government to ensure that the Turkish Energy company won its bid to build and operate

the power plant. In April 2015, Berko and the conspirators discussed paying $1 million to the Minister of Power who was responsible for securing key approvals enabling the project to progress.

Bribes were also paid to five Ghanaian officials during an all-expenses-paid trip to Turkey to view equipment for the power plant, during which the officials each received $5,000.

After the power plant deal was ratified by the Ghanaian parliament in July 2015, Berko and his co-conspirators emailed about their bribe payments at length. The evidence further detailed tens of thousands of dollars in bribes that Berko had personally paid and for which he was still owed.

To conceal the scheme from Goldman Sachs and others, Berko lied to Goldman's compliance team that was responsible for vetting the deal and he used his personal, non-official-business email account when talking about the bribes.

Berko and his co-conspirators also concealed and laundered the bribe payments using shell companies, sham invoices, nominee account holders and cash withdrawals. Payments in furtherance of the bribery scheme were laundered through U.S. and foreign bank accounts, including several in Berko's name. Goldman ultimately withdrew from the deal due to corruption concerns. (Source)

Employee Sentenced To Prison For $950,000+ Ghost Employee Fraud Scheme Against Employer - August 25, 2026

Between 2015 and 2020, Karan Gupta, 48, led a scheme to defraud his employer, Optum, Inc., by creating a no-show job for his lifelong friend, Shangraf Kaul, 45, as a data engineering manager and pocketing over half of Kaul's salary as a kickback.

Gupta, who was a senior director at Optum, hired Kaul to work on his team in late 2015, despite Kaul's lack of qualifications for the position. For over three years, Kaul performed no work at Optum while collecting a six-figure salary. Gupta, as Kaul's supervisor, facilitated Kaul's no-show employment and demanded Kaul pay him approximately 60% of his unearned salary in kickbacks. Gupta then devised a plan for him and Kaul to conceal the kickback payments, first through cash deposits into Gupta's own bank account, then through a designated checking account to which Gupta had access.

Gupta's fraud was ultimately discovered by Optum after his termination from the company in November 2019 for engaging in a similar no-show employee fraud. Optum investigated and referred the case to federal law enforcement. In total, Gupta's fraud against Optum totaled more than $950,000. Gupta's co-conspirator, Kaul, pleaded guilty on February 26, 2025, to one count of conspiracy to commit wire fraud and is currently awaiting sentencing. (Source)

Employee Pleads Guilty To Making $510,000+ Fraudulent Charges On Employers Credit Cards - July 30, 2026

Jeffrey Jeffers, 35, admitted to stealing $510,465.19 from his employer through false charges to company-issued credit cards.

Between November 2022 and July 2024, Jeffers delivered products by truck for a large provider of industrial gas from its distribution facility in Wood County, West Virginia.

The delivery trucks were fueled at the distribution facility and were also equipped with fuel credit cards. Jeffers admitted that he fraudulently charged a total of $510,465.19 in fuel costs to the credit cards throughout his term of employment.

Jeffers further admitted that the fraudulent credit card payments went to accounts for fictitious service stations he created on online payment processing platforms. Jeffers admitted that his delivery routes normally never required any refueling outside of the distribution facility. (Source)

Escrow Officer For Title Company Sentenced To Prison For Theft Of $460,000+ - August 13, 2026

Tracy Kellerstrass, 52 is the former escrow officer for Cameron Title Company in Missouri.

Kellerstrass previously pleaded guilty to bank fraud on March 24, 2026, and admitted to forging another employee's signature on numerous company checks and presenting them for deposit into her personal bank account. She will also be required to pay restitution for her theft of $460,415.84. (Source)

Office Manager Sentenced To Prison For Stealing $258,000+ From Business - August 27, 2026

Brittaney Hall, 37, worked as an office manager and accountant for a business in Martinsburg, West Virginia giving her access to accounts and financial information for the company.

Hall caused overpayments of payroll in reimbursements and commissions for her own benefit, wrote checks to herself without authority, and created false invoices which caused unauthorized payments to be made in her name. Hall was ordered to pay $258,143.51 in restitution. (Source)

Employee Charged With Stealing $150,000+ From Employer - August 3, 2026

An employee at a local kennel company is facing felony charges after she was accused of stealing over $150,000 from the company. Investigators say Jennifer Caulkin was serving as the general manager for Paradise Kennels when she was accused of stealing over $150,000 between Sept. 2023 and Feb. 2026. The incident report states the owners began investigating after bank deposits and register slips did not match. During the investigation, the owners learned Caulkin was also falsifying her hours and paying herself unauthorized overtime. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY BECAUSE OF FINANCIAL PROBLEMS, FOR PERSONAL ENRICHMENT, TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING ADDICATIONS

Employee Sentenced To Prison For Embezzling $26 Million+ From Employer With Help Of Boyfriend / Used Fund To Live In Mansions, Drive Luxury Cars, Etc. - July 30, 2026

From January 2018, to February 2025, Cynthia Marabella and her boyfriend co-defendant William Costa devised a scheme to defraud Marabella's employer, a Las Vegas construction company. As part of the scheme, they: fraudulently duplicated bonus checks and deposited the checks into bank accounts controlled by Marabella and Costa; opened credit cards in other peoples' names and made unauthorized charges then paid the credit cards' bills with stolen funds; provided false accounting records to the employer; created forged and false bank statements; and sent fictitious invoices from merchant accounts then paid the invoices with stolen funds.

Marabella and Costa used the stolen money to live in lavish mansions, to drive high-end cars, and to pay private school tuition. Marabella purchased high-end merchandise using the stolen funds and sold those items through an online consignment company. As a result of the fraud scheme, Marabella and Costa obtained more than $26 million from the employer. (Source)

Company Finance Director Sentenced To Prison For Embezzling $10 Million+ Over 16 Years / Used Funds To Pay For Credit Card Debit, Unauthorized Bonuses, Etc. - August 12, 2026

Mark Latham, 61 accepted a Finance Director role at his company in 2009 and began embezzling from the company by paying his personal credit card debt with company funds, providing himself unauthorized bonuses, paying for a relative's apartment with company funds, and directing company funds to his personal bank account.

Latham continued this conduct until he was caught in 2025. He concealed his conduct by editing the company's bank statements to remove payments to himself. Latham used the funds to lead a lavish lifestyle, including spending $39,000 on Super Bowl tickets in 2023, $29,731 on Taylor Swift concert tickets in 2023 and 2024, $46,248 for a room at the Four Seasons Hotel in Costa Rica in 2018, $38,827 on NFL season tickets from 2022 through 2024, and $28,098 on a golf simulator in 2024. In total, over the 17 years, Latham embezzled $10,752,535 from his employer and pay restitution to his employer. (Source)

Employee Pleads Guilty To Stealing $7 Million+ From Employer Over 12 Years / Used Funds To Pay Credit Cards, Vacations, Etc - August 11, 2026

Ricardo Fontanilla, 66, a dual national of the United States and the Philippines was charged and has agreed to plead guilty to stealing more than $7.1 million from his employer over the course of a decade.

Between 2013 and December 2025, Fontanilla worked at a global financial services company which had its U.S. headquarters in Massachusetts, as a Security Administration Services employee. Fontanilla's role allegedly gave him access to the company's financial systems, which tracked borrowers' mortgage payments in connection with residential mortgage-backed securities – a kind of financial instrument that allows investors to purchase ownership in a pool of residential mortgage loans.

Beginning in 2013, Fontanilla allegedly altered the company's records to make it appear that the company was receiving excess payments from mortgage servicing companies that were collecting borrower payments. Fontanilla fraudulently transferred these supposedly "excess" payments back to one mortgage servicer, and then falsely informed the company representatives that the his company had mistakenly refunded these amounts. In directing the mortgage servicing company to return the mistaken refunds to the his company, Fontanilla allegedly directed the mortgage servicing company to wire the funds to a personal bank account he controlled at Wells Fargo.

Records obtained during the investigation show Fontanilla allegedly received more than $7.1 million in wires from the mortgage servicing company between 2013 and 2025, and that Fontanilla allegedly made payments from his accounts of more than $4.78 million in personal credit card payments to Capital One, JPMorgan Chase, Wells Fargo and American Express; $873,000 in mortgage and loan payments; more than $200,000 in cash and cash-equivalent withdrawals in the United States and abroad; at least $300,000 in deposits to brokerage accounts at JPMorgan Chase; and approximately $125,000 in payments to Toyota – amounts far exceeding the approximately $83,000 annual salary Fontanilla received from the Victim Company. According to court documents, Fontanilla's spending included substantial purchases of luxury brands and premium air travel through the United States, the Caribbean and Asia. (Source)

Chief Financial Officer Charged / Pleads Guilty To Defrauding Hedge Fund Of $3 Million+ / Sued Funds For Adult Entertainment & Vacations - August 11, 2026

Beginning shortly after he began working for the fund and continuing until his termination in March 2026, Theodore Woo embezzled millions of dollars from the fund through a series of fraudulent transactions, including making millions of dollars in fraudulent payments to entities controlled by Woo and spending thousands of dollars on unauthorized personal expenses using credit cards paid by the fund.

As the CFO, Woo handled back-office tasks for the fund and had the authority to authorize the fund's administrator to process reimbursement requests. In that capacity, Woo instructed the fund administrator to make millions of dollars in payments to two entities, TWDRR LLC and MGTW LLC, for claimed "Research Consulting Services." Woo also sent invoices from those two entities that falsely represented that they had rendered services for the fund. In actuality, Woo controlled both entities, and neither entity had performed any service for the fund.

To further conceal his theft, Woofalsely claimed to the fund's external auditor that MGTW LLC was an independent research consulting firm engaged by the fund to develop short investment ideas on a project-by-project basis.

Woo also had the authority to effectuate transfers of cash from the fund to third parties, as the CFO. Over the course of his employment with the fund, Woo caused over 100 fraudulent transfers from the fund to a corporate entity controlled by WOO and to bank accounts in WOO's name.
Finally, while serving as CFO, Woo opened and controlled multiple credit cards in the name of the fund, and charged unauthorized personal expenses to those cards, including thousands of dollars in charges to adult entertainment establishments and international vacations. (Source)

Company Executive Director Sentenced To Prison For Embezzling $1.3 Million+ From Employer / Used Funds For Travel & Gambling - August 26, 2026

Justin Marquardt, 55, held the title of executive director at his employer's company and by virtue of his position, had access to all company finances and financial accounts from 1994 to 2023.

Marquardt previously admitted that he stole $1,387,926.39 from his employer's bank accounts and used those funds for his personal benefit. As part of his scheme, Marquardt, without authorization, transferred funds from his employer's bank accounts to his personal accounts and wrote himself unauthorized checks from business bank accounts. Marquardt spent most of the money on personal expenses, including travel and gambling both online and at casinos. To hide his embezzlement, Marquardt omitted these unauthorized transactions from the business's QuickBooks ledger he provided to an accountant and tax preparer. Marquardt recorded false and fraudulent payments as business expenses in the QuickBooks records to conceal his embezzlement. Marquardt has been ordered to pay $1,387,926.39 as restitution to his former employer. (Source)

Employee For Non-Profit Organization Sentenced To Prison For Theft Of $426,000 Of Federal Funds Over 7 Years / Used Funds To Pay Family Members, Etc. - August 27, 2026

Jodi Spargur-Tate, 55, was employed by Children and Families of Iowa (CFI) between 2015 and 2022 as a Program Director overseeing CFI's youth, adult, and dislocated worker programs.

During her time as Program Director, Spargur-Tate submitted hundreds of false and fraudulent reimbursement requests, including falsified invoices and receipts. She also diverted over one hundred payments from CFI to herself and her family members to pay their cell phone bills and housing costs, among other things. Spargur-Tate was ordered to pay $426,837.11 in restitution. (Source)

Company Bookkeeper Sentenced To Prison For Embezzling $291,000+ / Used Funds To Pay For Personal Expenses - August 7, 2026

Kathleen M. Michaelis, 50, was sentenced to 2 years in prison, followed by 2 years of supervised release, for five counts of wire fraud. Between May 2017 and May 2024, Michaelis was employed as a bookkeeper for a business in Christian County, Kentucky. She embezzled money from her employer utilizing a fraudulent check scheme. She used the stolen money to pay personal expenses. Michaelis concealed her scheme by failing to forward employee paystub withholdings to the United States Treasury and the company's retirement plan. Michaelis was also ordered to pay $291,470 in restitution. (Source)

Company Bookkeeper Sentenced To Prison For Stealing $253,000+ - August 26, 2026

Isha Warr, 53, worked as a bookkeeper for a small business in Lexington County in South Carolina from June 2023 to July 2024.

Shortly after starting work, Warr convinced the business to change their accounting software to a new system. The new software enabled Warr to pay money directly to herself, rather than paying company invoices. The business later discovered a series of unauthorized payments and unpaid invoices during a routine financial review. With the assistance of a forensic accountant, the business discovered a total of $253,855.48 in unauthorized transfers were made from the business account into Warr's personal account. (Source)

West Virginia Division Of Labor Administrative Services Manager Sentenced To Prison For Embezzling $18,000+ Using State Credit Cards / Used Funds To Pay For Personal Expenses - August 18, 2026

Kelli Rucker, 48, was hired by the West Virginia Division of Labor as an Administrative Services Manager in 2020 and assigned three state purchasing credit cards.

From 2022 through February 2023, Rucker fraudulently made unauthorized purchases with the three cards that resulted in losses totaling $18,472.75 to the State of West Virginia. As part of her guilty plea, Rucker admitted that she knew she was not permitted to make personal purchases with a state-issued card and that she electronically paid personal expenses including gas and electric bills, hospital expenses, and cable television bills as part of her fraudulent scheme. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL THEIR EMPLOYERS MONEY TO SUPPORT THEIR PERSONAL BUSINESS

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Bridgestone Tire Assistant Treasurer Pleads Guilty To $14 Million+ Fraudulent Shell Company & Invoicing Scheme / Used Funds For Investments - August 11, 2026

Sajju Khatiwada, 45, worked at Bridgestone's corporate headquarters in Nashville Tennessee from April 2016 until April 2024, most recently as Assistant Treasurer, Capital Planning and Funding. As part of his work in Bridgestone's Treasury Operations Department, Khatiwada managed the company's relationships with banks that provided credit card processing services for Bridgestone retail locations across the United States.

In July 2020, Khatiwada created a fictitious vendor, named Paymt-Tech, LLC, registered the company in Nevada under the name of an acquaintance, and opened bank accounts in the fictitious vendor's name.

On a monthly basis spanning nearly four years from August 2020 to April 2024, Khatiwada sent fraudulent invoices via email to other Bridgestone employees, falsely representing that Bridgestone owed Paymt-Tech money for purported "service charges." But Paymt-Tech performed no services for Bridgestone, and Khatiwada was not entitled to any of the money.

Relying on the fraudulent invoices, Bridgestone paid a total of $14,923,978.57 into Paymt-Tech accounts controlled by Khatiwada. Khatiwada transferred the fraud proceeds into financial and investment accounts under his control, where the money generated more than $6.1 million in interest, dividends, and other gains. In his plea agreement, Khatiwada admitted that the scheme generated approximately $21 million in total unlawful proceeds and agreed to forfeit that amount to the United States. He also owes restitution to Bridgestone totaling $14,923,978.57, plus interest, with the final amount to be determined by the court. (Source)

EMPLOYEES WHO EXTORT THEIR EMPLOYERS FOR MONEY, OR THREATENED DAMAGES OR THE RLEASING OF SENSITIVE INFORMATION

Data Analyst Sentenced To Prison For Extorting Employer For $2.5 Million When He Found Out That His Contract Was Not Being Renewed - August 13, 2026

Cameron Curry, 27, is being sentenced to prison for carrying out an extensive cyber extortion scheme against a D.C.-based international technology company.

Curry was contracted to work as a data analyst for approximately six months with the victim company. In that capacity, Curry had access to the victim company's data files and other personnel and corporate information.

Trial evidence established that Curry misused his position to access the victim company's personnel and other sensitive corporate records, which he then used to carry out the cyber extortion scheme. Curry hatched his extortion scheme after he learned that his contract was not going to be renewed and that he would no longer be employed by the company.

From Dec. 11, 2023, to Jan. 24, 2024, Curry, identifying himself online as "Loot," sent over 60 email messages to company employees and executives, threatening to disclose sensitive information unless he was paid $2.5 million dollars in cryptocurrency. Trial evidence further established that the email messages contained threats to disclose sensitive corporate information and employee data, including employees' personally identifiable information (PII), as well as threats to harm the reputation of the victim company by reporting a breach of its information and publishing the information publicly if the victim company failed to pay him via cryptocurrency.

On Jan. 24, 2024, the FBI executed a search warrant at Curry's residence, seizing various electronic devices. A forensic analysis of the evidence revealed that Curry was committing the extortion scheme under the "Loot" alias. (Source)

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

No Incidents To Report)

THEFT OF ORGANIZATIONS ASSESTS / DESTRUCTION OF PROPERTY

Employee Pleads Guilty To Stealing & Selling $4 Million Worth Of Company Products - August 27, 2026

From approximately November 2019 to March 2025, Paul Kroes, 42, engaged in a scheme to embezzle approximately $4 million from his employer, a retailer of transport temperature control systems for refrigerated trucks and containers. Since 2007, Kroes held several different roles and a variety of responsibilities at his company, and his last role was as a Product Manager.

Kroes abused his positions and sold his company products to third-party buyers and misappropriated the proceeds for his own personal benefit. Kroes would pull the products himself, or directed another employee to do so, and disguised the missing items from the company's inventory. Kroes had no authority to sell the products and concealed the payments he received through selling the embezzled products. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Company Financial Manager Sentenced To Prison For $18 Million Loan Fraud Scheme In Collusion With Sister & Brother in Law - July 31, 2026

Christine Gendron, 62, is a former certified public accountant. Gendron was also ordered to pay $392,607 in restitution for bank fraud, her apportioned share of the total loss. In June 2025, Gendron pleaded guilty to one count of conspiracy to commit bank fraud.

Gendron engaged in a conspiracy to commit bank fraud along with her sister, Jeanette Norman, and brother-in-law, Louis Masaschi, defrauding commercial lenders on multiple occasions. Together, they provided false and fraudulent rent rolls and forged lease agreements for numerous properties located in Springfield, Mass.; East Longmeadow, Massachusetts and Enfield, Connecticut.

Gendron worked as the financial manager for Norman and Masaschi at LL Realty Developers, LLC, an umbrella company which owned primarily commercial and some residential property in Western Massachusetts, Connecticut and elsewhere.

The three conspired with each other to fraudulently obtain loans from financial institutions and commercial lenders by providing materially false, fictitious and fraudulent financial information – including false rent rolls and forged lease agreements.

After receiving the loans, they defaulted on the loans, causing substantial losses to the financial institutions and commercial lenders, including two community credit unions, and leaving the buildings vacant.

Between May 2016 and November 2018, the coconspirators fraudulently obtained or sought to obtain approximately $60,123,000 in loans and caused a total loss of $18,203,030. (Source)

Washington Metropolitan Area Transit Authority Train Operator Sentenced To Prison For Role In $362,000+ Fraud / Kickback Scheme With 6 Other Employees - August 4, 2025

Michelle Shropshire, 55, worked as a train operator for the Washington Metropolitan Area Transit Authority (WMATA). For about four years, Shropshire orchestrated a scheme in which she and numerous WMATA employees submitted fraudulent disability and health care claims to AFLAC, claiming injuries they never suffered.

Shropshire prepared and submitted the fraudulent claims on behalf of herself and her co-conspirators, fabricating medical records and forging the signatures of real doctors to support the false claims. She and her co-conspirators continued to work and collect their regular WMATA paychecks throughout the periods they claimed to be disabled.

In exchange, each co-conspirator paid Shropshire a kickback of about 20 percent of the fraudulent insurance payout. Shropshire was responsible for defrauding AFLAC of at least $362,035.14, and personally profited by about $80,520.36.

Codefendant Jones pleaded guilty to the same conspiracy charge and is scheduled to be sentenced Aug. 6, 2026. 6 other WMATA employees have also pleaded guilty to related health care fraud offenses arising from the investigation. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Los Angeles International Airport Employee Charged With Possessing 24 Pounds Of Fentanyl - August 24, 2025

An employee of a service provider working at Los Angeles International Airport (LAX) and a resident have been arrested and charged in a federal criminal complaint with possessing a bag containing approximately 11 kilograms (24.3 pounds) of fentanyl in an airport bathroom, where it was to be taken and transported on a Minnesota-bound flight.

Miguel Angel Tuz-Noh, 24, of Lennox, who works at LAX, and Anthony Olvera, 23, also of Lennox, are charged with possession with intent to distribute a controlled substance.

Tuz-Noh law enforcement believes has ties to a drug trafficking organization. On August 19, law enforcement observed Tuz-Noh and Olvera attempt to exchange narcotics in a men's bathroom at one of the airport's terminals.

Soon afterward, law enforcement detained both defendants and opened a duffle bag Olvera had carried. Inside the duffle bag were 10 brick-type packages containing a total of approximately 11 kilograms of fentanyl. Law enforcement believes Olvera had agreed to fly with the fentanyl to Minneapolis-St. Paul International Airport. (Source)

OTHER FORMS OF INSIDER THREATS

Hong Kong Airlines Employee Sentenced To Prison For Accepting Bribes To Help Smuggle Mainland Chinese Travelers Overseas - July 29, 2026

A former customer services officer with Hong Kong's Cathay Pacific has been jailed for one year and eight months for accepting at least HK$18,000 (US$2,295) in bribes to help smuggle mainland Chinese travelers overseas 17 years ago.

Tsui Ying-kit, 45, pleaded guilty on Wednesday to four counts of conspiracy for an agent to accept advantages at Tsuen Wan Court, which now handles District Court cases. The defendant had been on the run since jumping bail in October 2009, before returning from mainland China to surrender in July last year.

In 2009, the Independent Commission Against Corruption arrested Tsui and two other Cathay customer services officers for accepting bribes to ensure an unspecified number of ineligible mainland passengers could check in for their flights and go through security checks between September 2008 and August that year.

The watchdog also arrested two men who acted as escorts accompanying the travelers to check in at Hong Kong International Airport.

A prosecution summary said Tsui had accessed Cathay's computer system to check flight information and security details so that the travellers he intended to smuggle overseas could receive their boarding passes without complication. (Source)

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

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES' EMPLOYEES' INVOLVED IN TERRORISM

Costco Employee Kills Co-Worker - August 11, 2026

A Costco employee in a Seattle allegedly rammed his car into a co-worker riding a motorcycle, killing him out of anger and jealousy, according to reports citing statements made to investigators.

Tyler Sorensen, 22, is charged with second-degree murder in connection with the July 31 death of 20-year-old Jonathon Langdon. Sorensen allegedly followed Langdon out of a Costco parking lot before swerving into his lane and striking his motorcycle. Langdon was thrown from his motorcycle into a metal signpost. Sorensen fled the scene but returned an hour later with a family member to speak with investigators. Sorensen told his father that he "did something stupid" and had been in a collision but kept going. Once his father realized that Sorensen had left the scene of an accident, he drove his son back to the collision site an hour after the deadly incident, prosecutors said.

Sorensen allegedly told investigators that he became jealous after seeing Langdon hug a female co-worker whom Sorensen claimed was his girlfriend. After seeing the hug, he texted friends that his "blood is boiling."

Sorensen allegedly told investigators that he and the female co-worker had been in a relationship for about two to three months, which ended in late May. However, she told police that they had never dated and that she only considered him a friend and had repeatedly told him she "needed space" and that he was "crossing boundaries," authorities said.

Sorensen allegedly told law enforcement that his actions were "stupid" and that he only wanted to "spook" Langdon. (Source)

U-Haul Worker Shoots & Kills Co-Worker After Argument - August 13, 2026

A Nashville U-Haul employee allegedly gunned down his 56-year-old co-worker during a shift, as police say he fired several shots after the two men were arguing over a drink.

Devin Rice, 23, was arrested on Aug. 5 after he allegedly shot and killed Fredrick Lytton at a U-Haul store in Nashville, Tennessee, according to police. Lytton died after arriving at Vanderbilt University Medical Center. (Source)

Fast Food Employee Admits Shooting At Customer / Will Be Sentenced To Prison - August 19, 2026

Tony Robinson, 28, pleaded guilty in to one count of being a felon in possession of a firearm. He admitted that on Dec. 17, 2025, he got into an argument with a customer of the fast-food restaurant where he was working. After a manager intervened, Robinson walked away from the drive-thru window and put his headset on the counter. The customer was standing outside, looking through the window of the dining room. Robinson then walked outside with a hand in his pocket. The customer backed up and opened fire.

Robinson pulled a gun from his pocket and returned fire. Both men continued shooting as they fled. The customer ran away and Robinson went back inside before firing through the window of the restaurant's dining room.

Robinson ran from the restaurant into a nearby church and hid his gun in a stairwell. When St. Louis Metropolitan Police Department officers found Robinson, he initially lied and said he threw his gun into a sewer. Officers found his gun, a .45-caliber Glock pistol. Police interviewed the customer, who also said he was acting in self-defense. Officers found four .45-caliber cartridge casings and nine 9mm casings. There were bullet holes in the windshield and hood of the customer's car and in the restaurant window. (Source)

Note:
There are any incidents like this. Why do fast food restaurants allow their employees to carry guns?

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
www.insiderthreatincidents.com

INSIDER THREATS DEFINITION / TYPES

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 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

The information complied below was gathered from research conducted by NITSIG.

INSIDER THREAT (Simplistic)

Insider Threat - The potential for an individual who has or had authorized access to an organization's critical assets (Facilities, Financial Assets, Employees, Data, Computer Systems - Networks) to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

INSIDER THREAT (Expanded)

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees (**1** - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (**2** - Failure By Action, Behavior Or Response) (**3** - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- ☐ Opportunist Employees (**1** - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (**2** - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (**3** - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- ☐ Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- ☐ Employees Involved In Foreign Nation State Sponsored Activities (Recruited - Incentives)
- ☐ Employees Ideological Causes (Promoting Or Supporting Political Movements To Engage In Activism Or Committing Acts Of Violence In The Name Of A Cause, Or Promoting Or Supporting Terrorism)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)
- ☐ AI Agents Taking Unintentional Or Intentional Requests That Violate The Organization AI Acceptable Use Policy
- ☐ Artificial Intelligence Agents That Can Act Without Human Oversight & Authorization (Sharing Sensitive Data, Making Decisions, Causing Harm, Etc.)

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

There can be many different types of Insider Threat incidents that are committed by employees as referenced below. While some of these incidents may take place outside the workplace, employers may still have concerns about the type of employees they are employing.

- ☐ Facility, Data, Computer / Network, Critical Infrastructure Sabotage By Employees (Arson, Technical, Data Destruction, Etc.)
- ☐ Loss Or Theft Of Employers Physical Assets By Employees (Electronic Devices, Etc.)
- ☐ Theft Of Data Assets By Employees (Espionage (National Security, Corporate, Research), Trade Secrets, Intellectual Property, Sensitive Business Information, Etc.)
- ☐ Unauthorized Disclosure Of Sensitive, Non-Pubic Information By Using Artificial Intelligence Websites Such as ChatGPT, Claude, MS Copilot, Google Gemini, Etc. Without Approval
- ☐ Theft Of Personal Identifiable Information By Employee For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial Theft By Employees (Theft, Stealing, Embezzlement, Wire Fraud - Deposits Into Personal Banking Account, Improper Use Of Company Charge Cards, Travel Expense Fraud, Time & Attendance Fraud, Etc.)
- ☐ Contracting Fraud By Employees (Kickbacks & Bribes That Can Have Damaging Impacts To Employer)
- ☐ Money Laundering By Employees
- ☐ Fraudulent Invoices And Shell Company Schemes By Employees
- ☐ Employee Creating Hostile Work Environment (Unwelcome Employee Behavior That Undermines Another Employees Ability To Perform Their Job Effectively)
- ☐ Workplace Violence Internal By Employees (Arson, Bomb Threats, Bullying, Assault & Battery, Sexual Assaults, Shootings, Deaths, Etc.)
- ☐ Workplace Violence External (Threats From Outside Individuals Because Of Relationship, Marriage Problems, Etc.) Directed At Employee(s))
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees Involved In Drug Distribution
- ☐ Employees Involved In Human Smuggling, The Possession / Creation Of Child Pornography, The Sexual Exploitation Of Children

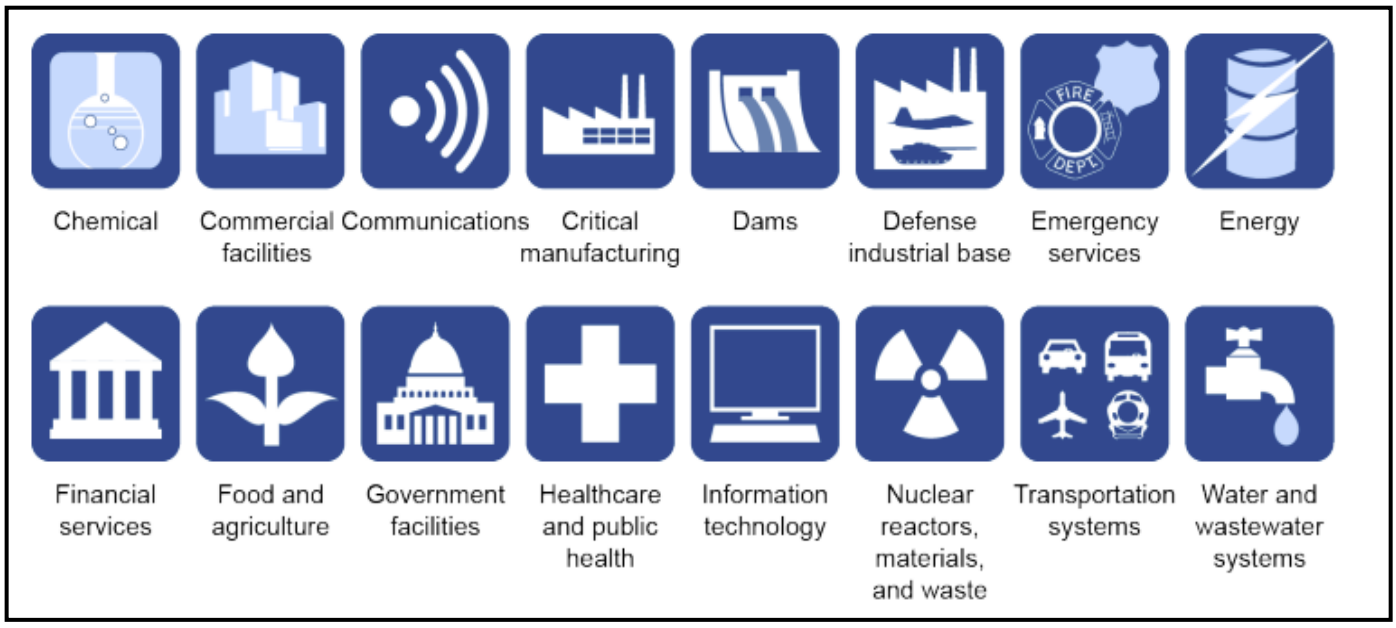
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ Stock Price Reduction
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss, Devaluation Of Trade Names, Loss As A Leader In The Marketplace
- ☐ Compliance Fines, Data Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees / Lawsuits
- ☐ Increased Distrust / Erosion Of Morale By Employees, Additional Turnover
- ☐ Employees Lose Jobs, Company Downsizing, Company Goes Out Of Business

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

NITSIG monthly Insider Threat Incidents Reports reveal that governments, businesses and organizations of all types and sizes are not immune to the Insider Threat problem.

- ☐ 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
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

An employer - employee relationship can be described as a circle of trust / 2 way street.

The employee trusts the employer to treat them fairly and compensate them for their work.

The employer trusts the employee to perform their job responsibilities to maintain and advance the business.

When an employee feels **This Trust Is Breached**, an employee may commit a **Malicious** or other **Damaging** action against an organization

Cultivating a culture of trust is likely to be the single most valuable management step in safeguarding an organization's assets.

After new employees have been satisfactorily screened, continue the trust-building process through on-boarding, by equipping them with the knowledge, skills and appreciation required of trusted insiders.

Listed below are some of the common reasons that trusted employees develop into Insider Threats.

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 Special Report: Employee Personal Enrichment Using Employers Money
Release Date: November 2025
You might be amazed at the many reasons employees steal money from their employers. Employees may not be disgruntled, but have other motives such as financial gain as outlined below.

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.) This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives. This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

What Do Employees' Do With The Money They Steal From Their Employers?
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 2026 REPORT ON FRAUD

If you manage or support an Insider Risk Management Program (IRMP), you should read this report. If there is someone else within the organization who is responsible for fraud, the IRMP Manager should be collaborating with this person very closely.

Could your organization rebound / recover from the severe financial impacts of a fraud incident?

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

Association of Certified Fraud Examiners 2026 Occupational Fraud Report Overview

This report to analyzes 2,402 real cases of occupational fraud that were investigated between January 2024 and September 2025. The findings presented in this report can be used by anti-fraud professionals, organizational management, and others to improve their fraud prevention, detection, and response efforts in several ways. These cases span organizations of all sizes, across a broad range of industries, and in every major geographic region.

As in prior editions, this report explores occupational fraud across six key dimensions: the methods by which frauds are committed, the financial impact of those schemes, the ways frauds are detected, the characteristics of victim organizations, the profiles and behaviors of perpetrators, and the outcomes of cases once misconduct is uncovered.

A primary goal of this report is to identify the frequency and cost of the various types of occupational fraud. Asset misappropriation schemes, or those in which an employee steals or misuses the employing organization's resources, were once again the most common category of occupational fraud, occurring in 90% of our study's cases and causing a median loss of USD $100,000, which was the lowest of the three categories.

Corruption was half as common as asset misappropriation, occurring in 45% of cases in the study and causing a median loss of USD $150,000. Although financial statement fraud, an intentional misstatement or omission of material information from the victim organization's financial reports, was the rarest form of occupational fraud (6% of cases), it was the most costly with a median loss of USD $1,000,000.

Types Of Organizations Impacted By Fraud

Private companies were victimized by the largest percentage of frauds in our study, accounting for 44% of cases with a median loss of USD $140,000. The least victimized organizations in our study were nonprofits 10%, which also incurred the lowest median loss USD $69,000. Government organizations fell in the middle of both spectrums, with 16% of cases impacting this category and a median loss of USD $110,000.

Fraud At Federal / State Levels

This report shows the majority of government organizations victimized by the frauds in our study were at the national level 37%, followed closely by local 32% and state / provincial 27% governments. National-level governmental organizations also suffered the highest median losses at USD $150,000, followed by state / provincial at USD $121,000 and local at USD $79,000. The significant and elevated fraud risk at the national level of government indicated by these results is likely related to the fact that national governments receive more funding and have complex organizational structures and operations, which could create more opportunities for occupational fraud.

The report provides a wealth of information on the types, sizes and industry of the victim organizations that experienced fraud, the perpetrators position, tenure, department, age, gender, education, etc. as referenced below. The report provides other information on collusion by employees, behavioral red flags of fraud, etc.
Download Report

REPORT INFOGRAPHICS
ACFE 2026 Occupational Fraud Report Key Findings
The Global Cost Of Fraud
Fraud In Banking & Financial Services
The Effectiveness of Providing Fraud Awareness Training
Profile Of A Fraudster
Collusion By Fruad Perpetrators
Behavioral Red Flags Of Fraud Perpetrators

Highlights Of The Association of Certified Fraud Examiners 2026 Occupational Fraud Report
This report provides undisputable evidence that collaboration between the Human Resources (HR) Department and the Insider Risk Management Program is critical, as referenced below. **(See Pages 69-70)**

Human Resources Red Flags
In addition to behavioral indicators, we asked whether perpetrators experienced job-related conditions that might have might have been a factor in their decision to commit fraud. These circumstances, referred to as HR-related red flags, include expressions of concern about job security, adverse performance evaluations, demotions, denial of raises or promotions, and reductions in compensation or benefits.

The report shows that 45% of perpetrators experienced at least one HR-related red flag prior to or during the fraud. The most commonly reported conditions were poor performance evaluations (12%), fear of job loss (12%), and being denied a raise or promotion (11%).

Behavioral Red Flags (BRF's) For Fraud
The report shows that 75% of fraudsters displayed at least one of the 8 most common behavioral clues listed below, and each of these BRF's were observed in at least 9% of cases. Fraudsters livening beyond their means has consistently been the most common behavioral red flag since we began tracking this data in 2008

39% Living Beyond Means
29% Financial Difficulties
17% Unusually Close Association With Vendor / Customer
12% Control Issues, Unwillingness To Share Duties
11% Irritability, Suspiciousness, Or Defensiveness
11% Bullying Or Intimidation
9% Wheel - Dealer Attitude
9% Divorce / Family Problem

Employee Background Checks
One of the most straightforward ways an organization can protect itself from fraud is to avoid hiring someone with a history of fraud-related misconduct. As such, effective background checks are an important part of a comprehensive fraud prevention program. This report showed that 64% of the victim organizations in our study conducted a background check on the perpetrator prior to hiring them, with 88% of those background checks coming back without any red flags.

However, 12% of the background checks did reveal at least one red flag before the perpetrator was hired, illuminating a gap in the protective value of background checks as an anti-fraud control. (**See Page 48**)

Hotline Reporting / Fraud Awareness Training

Organizations had 50% lower losses and 40% faster detection with a hotline. Whistleblowers are still the best detection method. Tips have been the most common detection method in every edition of this fraud report. (**See Page 51**)

Internal Control Weaknesses That Contribute To Fraud

Analyzing the root cause behind a fraud can help organizations both identify weaknesses that could lead to other violations and ensure that steps taken following the fraud truly remedy the factors that allowed it to occur. We asked respondents about the primary internal control weakness that contributed to the frauds they reported. This report showed 33% frauds occurred due to the victim organization lacking internal controls, with another 19% resulting from an override of existing internal controls. The next most common weakness cited was a lack of management review 18%. Collectively, these three weaknesses accounted for 70% of all frauds in our study. Other factors that contributed to fraud; Poor tone at the top 7%, Lack of competent personnel in oversight roles 7%, Other 6%, Lack of independent checks / audits 4%, Lack of employee fraud education 3%, Lack of clear lines of authority 2%, Lack of reporting mechanism <1%. (**See Page 49**)

Did Organizations Modify The Anti-Fraud Controls Following A Fraud Incident?

This report shows that 80% of organizations modified their controls following the detection of the fraud. Among the organizations that did modify their controls following the fraud, the most common changes pertained to management review, with 40% of victim organizations modifying their existing reviews and 37% implementing new reviews. More than half of the organizations also updated their approaches for data monitoring and analysis and for surprise audits. These three controls all focus on proactive fraud detection, indicating that victim organizations prioritized improvements in catching fraud faster and increasing the perception of detection among employees. (**See Pages 45-46**)

Perpetrators Position

According to our data, a perpetrator's level of employment within their organization correlated to the median loss and duration of the fraud. Frauds carried out by perpetrators at higher levels of authority caused higher losses and lasted longer, as has been the case in previous editions of this study.

This report showed that frauds carried out at the owner / executive level only represented 16% of the cases submitted but caused by far the highest median losses, at USD $475,000, which was more than nine times as much as employees USD $50,000, and more than three times as much as managers USD $125,000. Frauds carried out by employees and managers were much more common, each representing 41% of the cases submitted.

Similarly, perpetrators with higher levels of authority carried out fraud schemes that took longer to detect, according to our data. The median duration of frauds perpetrated by employees was only 8 months, just over one-third as long as those perpetrated by owners and executives (23 months); managers' frauds had a median duration of 14 months. (**See Page 51**)

Perpetrators Tenure With Employer

To assess how a perpetrator's employment tenure relates to occupational fraud risk, we asked survey respondents to report how long the primary perpetrator had been employed by the victim organization at the time the fraud occurred.

This report shows losses increased steadily with tenure, with schemes committed by individuals who had worked for the organization more than ten years resulting in the highest median losses USD $200,000. However, longer tenure did not equate to higher frequency; our findings indicate that, while extended tenure is associated with more-costly frauds, a majority of occupational fraud is committed by employees who have been employed at a victim organization fewer than five years. (**See Page 53**)

Schemes Based On Perpetrators Department

This report provides insight into the most common fraud schemes in high risk departments: Operations, Accounting, Sales, Customer Service, Executive / Upper Management, Administrative Support, Finance and Purchasing. (**See Pages 54-56**)

Perpetrators Position Based Gender

To further examine how gender relates to occupational fraud risk, we analyzed the frequency and median losses of frauds committed by male and female perpetrators across different levels of organizational authority. This report show female perpetrators were most frequently observed at the employee level, where they accounted for 36% of cases. Across all authority levels, frauds committed by females were associated with lower median losses than those committed by males. The greatest differences in both frequency and loss severity between genders occurred among owners and executives, indicating that gender disparities in fraud impact are most pronounced at the highest levels of authority. (**See Page 60**)

Perpetrators Age

Analysis revealed a clear relationship between a perpetrator's age and the financial impact of occupational fraud. This report shows median losses increased with age, with perpetrators over the age of 60 causing median losses of USD $850,000, which was more than 47 times greater than the median losses associated with perpetrators under the age of 26 USD $18,000.

Despite the high losses linked to older fraudsters, they accounted for a relatively small share of cases. Instead, perpetrators between the ages of 31 and 50 were responsible for the majority of frauds in our study, collectively accounting for 70% of reported cases. These findings indicate that, while fraud committed by older individuals tends to be more costly, occupational fraud most frequently originates from mid-career employees. (**See Page 61**)

Perpetrators Education Level

Analysis of perpetrators' education levels indicates that occupational fraud is most often committed by individuals with higher levels of formal education. More than 60% of the perpetrators in our study held at least a university degree. As illustrated in Figure 49, median losses increased consistently with higher levels of education, suggesting that perpetrators with greater educational attainment tend to cause more-costly frauds, likely reflecting their access to more-complex roles, responsibilities, or organizational resources .(**See Page 62**)

Collusion By Multiple Perpetrators

This report showed that in the fraud cases in our study, collusion was almost evenly split between those committed by a single perpetrator 51% and those involving two or more individuals acting together 49%.

Although collusive schemes occurred slightly less frequently than single-perpetrator frauds, they were associated with higher median losses than schemes carried out by one individual (USD $55,000). Losses increased further as the number of perpetrators grew, with frauds involving three or more individuals resulting in median losses more than twice as high as those involving only two perpetrators.

These findings suggest that collusion can significantly amplify fraud impact, likely due in part to the increased ability of multiple perpetrators to bypass anti-fraud controls when working together. (**See Page 63**)

Perpetrators Employment History / Criminal Background

Beyond criminal history, we also examined whether perpetrators had previously faced internal punishment for fraud-related conduct and, if so, where that action originated. This report shows prior discipline was uncommon among perpetrators in our study: 85% had no known history of fraud-related disciplinary action before the scheme occurred. Among the remaining cases, a small proportion involved individuals who had previously been terminated for fraud (6%), while others had received non-termination disciplinary sanctions (8%).

For perpetrators with a documented history of fraud-related discipline, responsibility for that action varied across employers. More than half had been disciplined by the same organization victimized in the reported case, while 33% had faced consequences at a previous employer. An additional 12% had been disciplined by both a former employer and the victim organization.

This report shows most perpetrators in our study had no known history of fraud-related criminal charges or convictions at the time of the offense. This finding suggests that traditional criminal background checks alone would not have prevented the majority of the frauds analyzed. Notably, however, 4% of cases involved perpetrators with a prior fraud conviction—either because that information was not identified during the hiring process or because it did not preclude their employment. These results highlight the limitations of relying solely on criminal history screening as a fraud prevention measure. (See Pages 66-67)

Internal Actions Taken Against Perpetrators

After a fraud examination has identified the perpetrator(s) involved in the scheme, the first step for most organizations is determining what internal punishments are appropriate and necessary. Termination is (and has been) the most common punishment, with 68% of perpetrators being terminated following the investigation of their fraud. A small portion of cases result in no punishment 4% or only a written or verbal warning 6%. (**See Page 73**)

Internal Punishment By Perpetrators Position

Within our survey responses, fraudsters can be found in every position in an organization. Their level of authority can affect the extent and impact of the fraud as well as the internal punishments they tend to receive. Owners and executives were terminated in only 52% of reported cases, while fraudsters working as managers 68% and employees 75% were more frequently removed. Similarly, owners and executives received no internal punishment for the fraud they perpetrated in 12% of cases, while managers and employees received no punishment more rarely 2% each. (**See Page 74**)

Litigation Against Perpetrators

Along with internal punishments, many organizations decide to pursue legal action against fraudsters. Private civil lawsuits and criminal referrals to law enforcement are the primary vehicles organizations use to pursue recoveries and punish fraudulent acts. We asked survey respondents whether the organizations victimized by fraud filed a civil lawsuit against the perpetrator and how the lawsuit concluded.

Organizations filed civil lawsuits in only 25% of reported fraud cases, though the suits that were filed were successful, either through a settlement or a judgment for the victim, in 82% of cases. (**See Page 75**)

Criminal Referrals Against Perpetrators

Fraud is a crime prosecuted by the government, but it's up to organizations to decide whether to refer cases they investigate internally to law enforcement. We asked survey respondents whether the victim organizations in their cases made a criminal referral, whether prosecution was pursued, and whether the prosecution was successful. Overall, organizations were much more willing to refer fraud cases for criminal prosecution compared to pursuing their own civil actions, with 54% of respondents reporting that the case was sent to law enforcement. Fraud prosecutions were generally successful, with 48% of defendants pleading guilty or no contest, 24% of defendants convicted at trial, and only 2% of defendants acquitted at trial. Most cases were pursued by law enforcement after being referred, with only 14% of respondents reporting that prosecutors declined to pursue the case. (**See Page 75**)

Reasons For Not Referring Fraud Case To Law Enforcement

Not all fraud cases are referred to law enforcement for further investigation and prosecution. To better understand the decision-making of the 46% of organizations who did not refer to law enforcement, we asked survey respondents what were the reasons. This report shows the most common response was that internal discipline was deemed sufficient punishment of the perpetrator 51%, followed by the fear of bad publicity 35% and private settlements being reached 20%. (**See Page 76**)

Recovering Fraud Losses

Organizations must weigh the benefits of internal punishments, costly legal actions, and settlement agreements against the potential for recovering assets lost to fraud. The results of our current survey and surveys past show an unfortunate trend of organizations failing to recover any fraud losses. This report showed 56% of the organizations in our study were unable to recover anything following the fraud. While 29% of organizations managed a partial recovery, only a small portion of respondents 15% reported a full recovery for the victim organization. (**See Page 77**)

Organization That Received Fines Because Of Employee Fraud

Organizations victimized by fraud might be fined or penalized by regulators in their jurisdiction due to the fraud uncovering or resulting from a compliance failure. We asked survey respondents whether the victim organization in their case had received such a fine and analyzed the results by scheme and the type of organization. This information can be helpful for organizations to understand how occupational fraud might result in a finding of noncompliance and help them make decisions concerning their internal compliance initiatives.

This report shows that 11% of organizations victimized by asset misappropriation schemes received a fine. Comparatively, in cases of financial statement fraud, 22% of victim organizations reported receiving a fine. Government agencies reported receiving fines most frequently 13%, while publicly traded companies received fines in the smallest percentage of cases 7%. (**See Page 78**)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

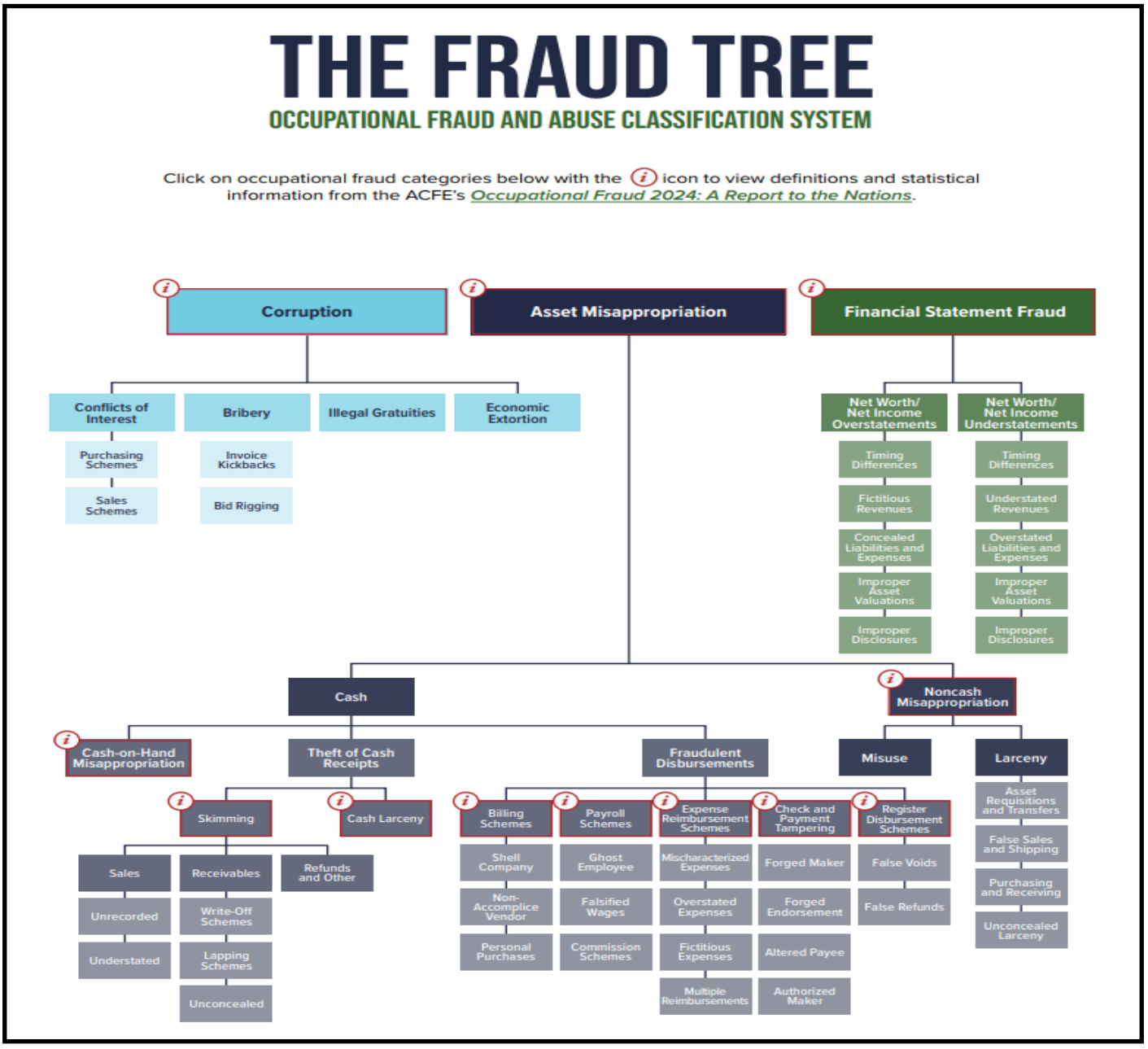
Other Tools

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

TD Bank Pleads Guilty To Money Laundering Conspiracy / Employees Accepted $57,000+ In Bribes / 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+ / GS Agrees To Pay $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)

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 Fraudulent 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)

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)

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 / DATA BREACHES

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)

South Korean Company Data Breach Caused By Employee Exposed Information On 34 Million Users / Company Must Compensate $1.1 BILLION To Affected Users - December 28, 2025

South Korean online retail giant Coupang said it will offer 1.69 trillion South Korean won ($1.17 billion) in compensation to 34 million users affected by a massive data breach disclosed last month.

The company said in a statement that it planned to provide customers with purchase vouchers totaling 50,000 won for various Coupang services. Former customers who closed their Coupang accounts following the data breach are also eligible to receive the vouchers.

Harold Rogers, interim CEO for Coupang Corp., described the move as a "responsible measure for our customers," and said the company would "fulfill its responsibilities to the end."

The data breach, which was revealed on Nov. 18, 2025 led to the resignation of CEO Park Dae-jun earlier this month.

Coupang founder Kim Bom said in a separate statement that the company had failed to communicate clearly from the outset of the incident. The U.S.-based chairman acknowledged his apology was "overdue," explaining that he initially believed it was best to communicate publicly and apologize only after all the facts were confirmed.

Kim added that the company has recovered all the leaked customer information through cooperation with the government, as well as the storage devices belonging to a suspect behind the data breach.

He also said the customer information stored on the suspect's computer was limited to 3,000 records and that it was not distributed or sold externally.

As the police continued their investigations in Coupang's offices, they uncovered that the primary suspect was a 43-year-old Chinese national who was a former employee of the retail giant. The employee had joined Coupang in November 2022, and was assigned to an authentication management system and left the firm in 2024. He is believed to have already left the country. (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)

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)

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)

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)

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)

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

Disgruntled Employee Charged For Setting Fire To 1.2 Million Square Foot Warehouse Causing Approximately $500 Million In Damage - April 9, 2026

A massive fire tore through a nearly 1.2 million-square-foot warehouse in Ontario, California, in the early hours of April 7, 2026 escalating into a six-alarm blaze that took hours to control. Flames and heavy smoke were seen billowing from the facility as more than a hundred firefighters rushed to the scene. The warehouse, which stored large quantities of paper-based consumer goods, suffered extensive damage, with parts of the structure collapsing as the fire spread rapidly. The fires Chamel Abdulkarim set quickly consumed the building, resulting in its destruction and causing approximately $500 million in damage.

Abdulkarim, a 29-year-old employee from Highland, California, worked at the facility through NFI Industries, a logistics partner for Kimberly-Clark. He is now accused of being responsible for starting the fire that destroyed a major distribution centre serving millions of consumers.

According to an affidavit filed with the federal criminal complaint, early in the morning on April 7, Abdulkarim filmed himself setting fire to multiple pallets of paper goods inside of a large distribution center in Ontario. As he lit the fires, he stated, "If you're not going to pay us enough to [expletive] live or afford to live, at least pay us enough not to do this [expletive]."

Abdulkarim posted videos of himself on social media setting the fires. He further made statements to others on the telephone and via text messages related to his motive for setting the building on fire, including the following: "I just cost these [expletive] billions," "1% is a [expletive] joke," and "All you had to do was pay us enough to live. Pay us more of the value WE bring. Not corporate. Didn't see the shareholders picking up a shift." (Source)

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)

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)

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)

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

NITSIG INSIDER THREAT SPECIALIZED REPORTS

The websites listed below are updated daily and monthly with the latest incidents.
There is NO REGISTRATION required to download the reports.

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 (**7,400+ 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 POSTINGS ON TWITTER / X
Updated Daily
https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

INSIDER THREAT INCIDENTS MONTHLY REPORTS
July 2021 To Present
http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SPECIALIZED REPORTS
Produced By:
National Insider Threat Special Interest Group (NITSIG)
Insider Threat Defense Group (ITDG)

Practical Guide For Securing Buy-In From CEO's & Stakeholders For Insider Risk Management Program / May 2026
The purpose of this guide is to put some clarity into describing the Insider Threat problem, the Return On Investment (ROI) for creating an Insider Risk Management (IRM) Program (IRPM) and eliminate the confusion that still plaques many organizations from developing or maturing their program.

IRMP's often lack CEO support because they are frequently misperceived as expensive, productivity-stifling, employee witch hunt programs that provide unclear ROI. These misconceptions are based on misinformation and false assumptions.

What will be described in this guide is a practical and real world approach to better educate the CEO and key stakeholders on having a more comprehensive understanding of the mission, scope and costs for an IRMP. The guidance in this document will focus on IRM from a 360 degree perspective, not just a technical perspective as many other guides do. (Download Report)

Employee Personal Enrichment Using Employers Money / November 2025
You might be amazed at the many reasons employees steal money from their employers.

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.)

This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives.

This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

Insider Threat Fraudulent Invoices & Shell Schemes Report / August 2025
Pages 6 to 24 of this report will highlight employees that are involved in **1)** Creating fraudulent invoices (For Products, Services And Vendors That Don't Exist) **2)** Manipulating legitimate invoices **3)** Working with external co-conspirators / vendors to create fraudulent or manipulated invoices.

These fraudulent invoices will then be submitted to the employer for payments to a shell company created by the employee, who will receive payment to a shell company bank account or through other methods. These fraudulent invoices schemes may happen just once or become reoccurring.

Employees may also collaborate with other employees, vendors or third parties to approve fraudulent invoices in exchange for kickbacks. An accounts payable employee might work with a vendor to create fraudulent invoices, and then the employee ensures the invoices are approved. Then the employee and vendor share the proceeds after the payment is issued.

These schemes can be disguised as legitimate business transactions, making them difficult to detect without proper internal controls. A shell company often consists of little more than a post office box and a bank account.

These schemes are often perpetrated by an opportunist employee, whose primarily focuses is for their own self-interest. They take advantage of opportunities (Lack Of Controls, Vulnerabilities) within an organization, often with little regard for the ethics, consequences or impacts to their employers. They are driven by a desire to maximize their personal financial gain.

From small companies to Fortune 500 companies, this report will provide a snapshot of fraudulent invoicing and shell companies schemes that are quite common.

This report and other monthly reports produced by the NITSIG provide clear and indisputable evidence that Insider Threats is not just as a data security, employee monitoring, technical, cyber security, counterintelligence or investigations problem

Why Insider Threats Remain An Unresolved Cybersecurity Challenge
Produced By: IntroSecurity: NITSIG - ITDG / June 2025
The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

This report provides detailed recommendations for mitigating Insider Risks and Threats. It outlines strategies for strengthening IRMP's and cross-departmental governance, adopting advanced detection techniques, and fostering key stakeholder and employee engagement to protect an organizations Facilities, Physical Assets, Financial Assets, Employees, Data, Computer Systems - Networks from the risky or malicious actions of employees.

The goal of this report is to provide anyone involved in managing or supporting an IRM Program with a common sense approach for identifying, deterring, mitigating and preventing Insider Risk and Threats. Through research, collaboration and conversations with NITSIG Members, and discussions with organizations that have experienced actual Insider Threat incidents, the report outlines recommendations for an organization to defend itself from the very costly and damaging Insider Threat problem. (Download Report)

U.S. Government Insider Threat Incidents Report For 2020 To 2024
The NITSIG was contacted by Senator Joni Ernst's office in December 2024, and a request was made to write a report about Insider Threats in the U.S. Government for the Department Of Government Efficiency (DOGE). (Download Report)

Department Of Defense (DoD) Insider Threat Incidents Report For 2024
The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. (Download Report)

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. (Download Report)

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS
https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed. The comprehensive reports and guidance provided by the NITSIG, quickly fueled the NITSIG memberships growth to become the largest U.S. / Global Insider Risk Management ISAC.

The NITSIG has been successful in bringing together a diverse group security professionals and individuals managing and supporting Insider Risk Management (IRM) Programs from the: U.S. Government Agencies, Department Of War, Intelligence Community Agencies, Critical Infrastructure Providers, Law Enforcement, 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 protecting their organizations assets against the severe impacts that can be caused by **Just 1 Employee**, **Multiple Employees In Collusion** or **Employees In Collusion With External Co-Conspirator(s)**. Many members have even stated the NITSIG is like having a team of IRM experts consultants at their disposal **FREE OF CHARGE**.

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;

- ✓ IRM Program (Development, Management, Evaluation & Optimization)
- ✓ IRM Program Working Group / Hub Operations
- ✓ Insider Threat Investigations & Analysis
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Vulnerability Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Employee Continuous Monitoring & Reporting Programs (Benefits, Guidance, Solutions)
- ✓ 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. The meetings are held at various locations throughout the U.S. See this link for some of the great speakers we have had at our meetings.

NITSIG Insider Threat Symposium & Expo (ITS&E)

ITS&E events (1 Day) provide attendees with outstanding speakers who have expert knowledge of developing, managing, evaluating and optimizing IRM Programs. The NITSIG has held 5 ITS&E events (2015, 2017, 2018, 2019 and 2025) at the Johns Hopkins University Applied Physics Laboratory, in Laurel, Maryland.

The ITS&E features expert speakers, engaging panel discussions, interactive sessions, vendor technologies and solutions, and networking with IRM practitioners. (2025 ITS&E)

NITSIG IRM Resources

Posted on the NITSIG IRM Website are various documents, resources and training that will provide guidance to assist organizations with their IRM / IRM Program efforts. The website is a public repository of documents containing guidance for IRM and security practitioners to use for expanding their knowledge of protecting their organizations assets against Insider Threats.

NITSIG LinkedIn Group

The NITSIG has created a LinkedIn Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with **950+** members enables 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.

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. AB members will provide oversight, educational, strategic and operational guidance to support the mission of the NITSIG, and also help to facilitate building collaborative relationships with individuals that manage or support IRM Programs.

Please contact me with any questions regarding the NITISG or IRM.

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The NITSIG
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
561-809-6800
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

Since 2009, the Insider Threat Defense Group (ITDG) has provided **700+** organizations and **1000+** students with the core skills / advanced knowledge, resources and technical solutions for developing, managing, evaluating and optimizing their organizations Insider Risk Management (IRM) Programs (IRMP's).

The ITDG exceeds IRM compliance regulations and help organizations create comprehensive, robust and cost effective IRMP's.

Being a pioneer in understanding Insider Risks - Threats from both a holistic, non-technical and technical perspective, the ITDG stands at the forefront of helping organizations safeguard their assets (Facilities, Employees, Financial Assets, Data, Computer Systems - Networks) from one of today's most damaging threats, the Insider Threat. **The financial damages from a malicious or opportunist employee can be severe, from the MILLIONS to BILLIONS.**

With 15+ years of IRMP expertise, the ITDG has a deep understanding of the collaboration components and responsibilities required by key stakeholders, and the many underlying and interconnected cross departmental components that are critical for a comprehensive IRMP. This will ensure key stakeholders are **universally aligned** with the IRMP from an enterprise / holistic perspective to address the Insider Risk - Threat problem.

IRMP TRAINING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRMP Stakeholders Training Course & Workshop / Table Top Exercises
- ✓ IRMP Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees
- ✓ Customized IRMP Training For Our Clients

CONSULTING SERVICES OFFERED

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

BACKGROUND ON ITDG EXPERTISE IN THE FIELD OF INSIDER RISK MANAGEMENT

Insider Risk Management Program 360 Framework & Assessment Methodology (IRMP360FAM™)

Since 2009, the ITDG has been involved in U.S. Government, Department of Defense (DoD) and Intelligence Community Agencies (ICA's) Insider Threat Program (ITP) efforts.

From 2009 to 2011, the ITDG was under contract with the DoD Insider Threat Counterintelligence Group (ITCIG) to provide guidance in various areas of IRM. The DoD ITCIG in collaboration with other agencies (NCIX - NCSC, NSA, CIA, NGA, NRO,) were instrumental in developing what is known as National Insider Threat Policy (NITP).

The ITDG Insider Risk Management Program (IRMP) Framework was initially developed in 2014 with the help of individuals managing and supporting ITP's for the DoD and ICA's.

The IRMP Framework has undergone several enhancements over the years and provides comprehensive guidance for IRMP Development, Management, Evaluation and Optimization, for both the U.S. Government and private sector businesses. It is continuously being evaluated and updated due to the ever changing Insider Threat landscape. The IRMP Framework is practical, real world, cost effective, proven, unique and holistic.

Since 2014, the IRMP Framework has served as the backbone for our training and consulting services. The ITDG is a visionary in the field of IRM. In 2014, the ITDG was one of the first companies to offer comprehensive ITP Development / Management Training to the U.S. Government and defense contractors, who were required to implement programs based of off NITP and the NISPOM Conforming Change 2 Regulation.

The IRMP Framework encompasses 11 critical domains for IRM and an IRMP. Our methodology addresses Insider risks and threats from an enterprise cross functional perspective, and from a non-technical and technical perspective. No one in an organization is positioned to see every single employee risk factor or behavioral indicator. Ensuring that enterprise security foundations are in place, and that there is universal alignment and collaboration with key stakeholders and the IRMP, is a critical element for detecting, responding to, investigating, preventing and mitigating Insider risks and threats.

Our IRMP Framework covers Insider Risk Management from A to Z, to enhance the security foundations of the organization, and to prevent operational disruptions, downtime, loss of productivity, loss of income, loss of assets, prevent workplace violence, legal exposure, etc. from the negligent, disgruntled, malicious and opportunist actions of employees.

The ITDG has empowered organizations with the ability to implement, manage and optimize a comprehensive and cost effective IRMP, transforming the Insider Threat problem from a siloed **REACTIVE** task into a shared **PROACTIVE** organizational responsibility.

CLIENT SATISFACTION / COMPANY RECOGNITION

The comprehensive nature of our IRMP Framework and 15+ years of IRMP expertise, is what separates us from other providers of IRMP training and consulting services. ITDG training courses have been taught to over **1000+** individuals. Our students and clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM.

Even our most experienced students that have attend our training courses, or taken other IRMP training courses and paid substantially more, state that they are amazed at the depth of the training content and the resources provided, and are very satisfied they took the training and learned some new concepts and techniques for IRM.

Our client satisfaction levels are in the **EXCEPTIONA**L range. You are encouraged to read the feedback from our clients on this link.

The ITDG Has Provided IRMP Training & Consulting Services To An Impressive List Of 700+ Clients:
White House, U.S. Capital Police, 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, Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. (Client Listing)

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.
IRMP Evaluation & Optimization Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Threat Vulnerability Assessor & Mitigation Specialist
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG