INSIDER THREAT INCIDENTS REPORT
FOR
April 2026

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 **7,000+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This is very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

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

To grasp the magnitude of the Insider Threat problem, one must look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to **significant underreporting** on the Insider Threat problem.

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

Some organizations invest 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 26** 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 APRIL 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

2 Israeli Air Force Technicians Charged With Spying On Behalf Of Iran, Providing Information On Fighter Jets & Military Facilities - April 23, 206

Two Israeli Air Force technicians were charged on with spying on behalf of Iran, including providing information on fighter jets and military facilities, Israeli authorities announced in one of the most serious incidents amid a wave of efforts by Tehran to recruit Israelis.

An indictment filed by military prosecutors on Thursday morning accused the pair, who served as F-15 aircraft mechanics at the IAF's Tel Nof Airbase, of a series of "security offenses on behalf of Iranian intelligence elements."

One soldier was charged with aiding an enemy in wartime, providing information to an enemy, facilitating contact with a foreign agent, and additional offenses. The second soldier was charged with contact with a foreign agent, providing information to an enemy, and other offenses. In a joint statement, the Shin Bet security agency, the IDF, and the police said that the two technicians claimed in their interrogation that contact with the Iranian handlers was severed after they refused to carry out tasks involving weapons.

"However, even after the contact was cut off at the initiative of the handler, they did not cease attempts to renew contact, for the purpose of financial gain," the statement said. Army Radio reported that when the contact began around a year ago, an Iranian handler asked one of the soldiers, "What monthly salary would satisfy you?" and the soldier replied, "$1,300." According to the indictment, over the course of several months, the two soldiers "maintained contact with Iranian intelligence elements and carried out various tasks under their direction in exchange for money." The indictment also said that one of the soldiers transferred to an Iranian agent "materials from his military training relating to fighter aircraft systems, as well as documentation of facilities and areas within a military base."

Eight other soldiers serving at the base were reportedly suspected of having known about the alleged espionage without reporting it. (Source)

Former Employee Of The Croatian Mission To The U.N. Charged With Embezzling $750,000 Through Fraudulent Invoicing Scheme - April 1, 2026

From July 2017 through November 2023, Renata Saltus worked at the Permanent Mission of the Republic of Croatia to the United Nations (PMRC) in a financial administrative capacity. By virtue of her position, Saltus had unique access to the PMRC's vendor payment systems and was authorized to submit and process invoices on the PMRC's behalf.

For 6 years Saltus used her access and position to carry out a fraudulent invoicing scheme to embezzle funds from the PMRC's accounts into her own personal bank accounts. Saltus carried out this scheme by at least two different means. Saltus sometimes made double payments for certain invoices, which typically involved an authorized payment to the vendor for the PMRC and then a second payment of the same amount to one of Saltus's own bank accounts. At other times, Saltus created fake invoices, sometimes from fictitious vendors and billed them to the PMRC, but then directed the fraudulent payments to bank accounts under her control.

In total, Saltus embezzled at least approximately $750,000 over the course of her fraudulent invoicing scheme and used the funds for her personal benefit. (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

Employee Pleads Guilty To Hiding The Fact She Was Working For 3 U.S. Government Agencies Simultaneously - April 1, 2026

From May 2022 through at least in or around April 2025, Nehemie Almonor, 41, electronically submitted timecards certifying that she had performed full-time work during overlapping hours for multiple entities, including a private company, the U.S. Transportation Security Administration, U.S. Department of Housing and Urban Development, U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Food and Drug Administration, and the U.S. Air Force Reserves. Almonor commonly submitted timecards for full-time work at three positions simultaneously, attesting to having worked 120 hours or more in single 40-hour periods.

Almonor, a human resources specialist, would commonly keep at least three work laptops open next to each other to falsely represent to her employers that she was online and working full-time solely for each of them. Over the course of being employed by at least three full-time positions simultaneously, TSA received multiple complaints that Almonor was commonly unreachable during the hours she was certifying on her timecards. While employed in various full-time telework positions at once, Almonor applied to other government agencies claiming to be unemployed and therefore available to start immediately. Almonor also claimed full-time work while on military orders with the U.S Air Force at the same time she claimed full-time work for three other entities. Almonor collectively defrauded her employers of at least $291,905. (Source)

U.S. House of Representatives Employee Pleads Guilty To Accessing To Congressperson's Bank Account & Stealing $22,000+ To Pay Credit Card Bills - March 31, 2026

Courtney Hruska, 40, was employed on the member's staff from August 2015 to January 2022. To fulfill part of Hruska's official duties and responsibilities, the member entrusted Hruska with the member's personal credit card and bank account information. On Jan. 30, 2022, Hruska left the office for a new position with a federal agency.

Without authorization, Hruska retained the member's personal credit card and bank account information. Between Aug. 19, 2023, and July 30, 2024, Hruska used the member's bank account information to make payments towards the balance of Hruska's own personal credit card bills on 10 separate occasions. The member did not use electronic banking and did not receive immediate alerts from the bank. Because more than a year had lapsed between Hruska's first fraudulent transaction and the member's discovery of the theft, the member recovered less than nine percent of the stolen funds in fraud compensation. In total, Hruska caused a loss to the Representative of at least $22,865. (Source)

2 U.S. Postal Workers Sentenced To Prison For Theft Of U.S. Treasury Checks Valued At $4 Million+ - April 14, 2026

Kevaughn Wellington and Ky-Mani Straker, each former United States Postal Service (USPS) employees, were sentenced to prison for their participation in a fraudulent scheme through which they sold, for their own financial gain.

From approximately June 2021 through August 2023, the defendants engaged in a scheme to steal and sell Treasury checks mailed for distribution through the JFK Mail Facility. Wellington, who was employed at the facility as a mail clerk, worked with others to steal parcels containing Treasury checks. Then, together with Straker and others, Wellington sold the stolen Treasury checks for a portion of the face value of each check. As part of the scheme, Wellington stole—and conspired with Straker to sell—over 125 Treasury checks valued at more than $4 million, including checks intended to be individuals' Social Security benefits, COVID relief and tax refunds. In addition to selling stolen Treasury checks, Straker falsely endorsed and deposited stolen Treasury checks into a bank account and withdrew the proceeds for his own financial gain. Law enforcement uncovered over 350 videos and images from Wellington's phone depicting Treasury checks that were not addressed to him or Straker. (Source)

Social Security Administration Employee Charged In $116,000+ Disability Funds Theft Scheme - April 17, 2026

Najee Alexander Corbett, 37, of Baltimore, Maryland is charged with wire fraud, mail fraud, aggravated identity theft, theft of government property, and false statements. Through his position, the former SSA customer service representative could access sensitive SSA databases containing benefit claimants' personally identifiable information.

Beginning in February 2023, and continuing through April 2023, Corbett willfully devised a scheme to defraud the SSA. Through the scheme, Corbett fraudulently obtained Supplemental Security Income (SSI) benefits, designated for other individuals, for his and his associates' personal use.

As part of the scheme, Corbett targeted SSI claimants diagnosed with mental health disorders. Corbett then altered claimant records in the database to include bank accounts he controlled and his residential mailing address to receive their SSI benefit funds.

Additionally, in furthering the scheme, Corbett changed the date of benefit eligibility payments for the selected claimants in SSA's database which generated back payments in the claimants' names. Corbett then caused claimants' SSI benefit payments to be transmitted to bank accounts he controlled and mailed to his home. Through the scheme, Corbett received $116,537.62 in SSI disability payments and retained $71,304.62. (Source)

U.S. Postal Service Employee Arrested For Stealing $620,000+ Worth Of Checks & Credit Cards From Mail To Pay For Gambling & Personal Expenses - April 13, 2026

Jimbert Escalicas began working for the U.S. Postal Service in September 2023. His duties included delivering mail to routes in Sacramento County.

From November 2023 through October 2024, Escalicas stole checks, gift cards, debit cards and credit cards from mail destined for Postal Service customers on his routes. Escalicas forged the account owners' signatures on checks he stole and altered checks to make them payable to himself. He then deposited the forged and altered checks into accounts he controlled. At times, Escalicas sold stolen checks to others. To activate and use the credit cards he stole, Escalicas contacted the issuing financial institutions and provided the card owners' personally identifiable information. Escalicas stole no less than 130 checks and cards with a total value of more than $620,000. (Source)

U.S. Post Office Employee Sentenced To Prison For Stealing Gift Cards, Cash & Checks Totaling $8,500+ From Mail - April 7, 2026

From approximately September 2022 through July 2023, Michael Murray worked as a USPS postal clerk at the Beach Street Post Office in Revere and the Melrose Post Office in Massachusetts.

From approximately April 2023 through July 2023, Murray used his official position to steal the contents of hundreds of pieces of mail entrusted to him, including gift cards, cash and checks totaling approximately $3,422. During the same time period, Murray stole and fraudulently negotiated USPS money orders by generating them for postal customers for his own use totaling approximately $5,131. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing Narcotic Medications For United States Military Veterans - April 14, 2026

Carrie Wallace used her position as a U.S. Postal Service employee to access and steal mail parcels containing prescription medication and vape products. She intentionally targeted packages sent by the Department of Veterans Affairs to its patients because those packages generally contained narcotic medications. Wallace cut into the packages, opened the prescription narcotics medication bottles, stole the medication and replaced it with over-the-counter medication, retaped the packages and placed them back in the mail stream to be delivered to the intended recipients.

Multiple veteran victims consumed the tampered medication, putting them at risk of injury for taking incorrectly dispensed drugs. Due to Wallace's medication theft and tampering, veteran victims experienced extreme pain, increased agitation, anger, and other mental health symptoms. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Air Force Master Sergeant Pleads Guilty To 9 Year $37 Million Contract Bid Rigging & Bribery Scheme That Defrauded USAF - April 2, 2026

A former active-duty Master Sergeant (Alan James), of the U.S. Air Force (USAF) pleaded guilty to fraudulently inflating the cost of information technology (IT) contracts for the U.S. Pacific Air Forces (PACAF) by at least $37 million and using the excess funds to enrich himself, enrich co-conspirators, and channel bribes to a federal public official in PACAF whom the conspirators nicknamed "Godfather."

From at least April 2016 until about April 2025, James and his coconspirators falsely inflated the cost of IT contracts. James and his coconspirators agreed to use the excess funds to pay James, James' family members, the family of an Air Force civilian employee, and other co-conspirators. As part of this scheme, the conspirators diverted government funds to pay for an all-expenses-paid multi-day stay at a luxury resort on the North Shore of Oahu in 2023. Also, from at least May 2019 until about October 2022, the defendant directed co-conspirators — who were supposed to be competitively bidding against one another to win government contracts — on the amounts they should bid to circumvent the competitive bidding process. As a result of the defendant's actions, the government overpaid for IT contracts by at least $37 million.
(Source)

U.S. Army Soldier Charged With Using Classified Information To Profit $409,000+ From Polymarket Prediction Market Bets - April 23, 2026

Gannon Van Dyke has been an active-duty soldier in the U.S. Army, stationed at Fort Bragg, a military base located in Fayetteville, North Carolina. Starting around December 8, 2025, and continuing through at least January 6, 2026, Van Dyke was involved in the planning and execution of Operation Absolute Resolve, a military operation to capture Maduro, and had access to sensitive, nonpublic, classified information about that operation.

In 2025, Polymarket, a prediction marketplace operated by Blockratize, Inc., began offering binary event contracts related to whether certain events involving Venezuela and/or Maduro would, or would not, occur. Those event contracts included the future likelihood of "US forces in Venezuela by" certain dates, the future likelihood of Maduro being "out" of or removed from power by certain dates, the future likelihood of the U.S. invading Venezuela by on or before January 31, 2026, and the future likelihood of President Trump "invokeing War Powers against Venezuela" by a certain date.

As alleged, on or about December 26, 2025, Van Dyke created a Polymarket account, funded it, and began trading on Maduro- and Venezuela-related markets. In total, Van Dyke made approximately 13 bets from December 27, 2025, through the evening of January 2, 2026. Those bets all took the "YES" position on "U.S. Forces in Venezuela . . . by January 31, 2026"; "Maduro out by . . . January 31, 2026"; "Will the U.S. invade Venezuela by . . . January 31,"; or "Trump invokes War Powers against Venezuela by . . . January 31." Van Dyke bet a total of approximately $33,034 on those outcomes while in possession of classified nonpublic information about Operation Absolute Resolve.

In the predawn hours of January 3, 2026, U.S. special forces apprehended Maduro and his wife at a residence in Caracas, Venezuela, and hours later the President of the United States announced the successful operation. Following the President's public announcement, Polymarket resolved several Maduro- and Venezuela-related contracts to "YES," including the markets "Maduro out by . . . January 31, 2026," and "US forces in Venezuela by . . . January 31, 2026." As a result, Van Dyke won his wagers on those contracts. In total, Van Dyke allegedly profited approximately $409,881. (Source)

U.S. Army Employee Charged With Leaking Top Secret Information To Journalist - April 8, 2026

Between 2022 and 2025, Courtney Williams repeatedly communicated with the Journalist via telephone and text messages. During this period, Williams and the Journalist had over 10 hours of telephone calls and exchanged more than 180 messages. In one such message, the Journalist identified themselves as a journalist and stated that they sought information about the Special Military Unit of the Army in support of an upcoming article and book.

After these communications with Williams, the Journalist published a book and article that named Williams as a source and attributed specific statements to her. Some of these statements contained classified national defense information. In addition to her disclosures to the Journalist, Williams also made unauthorized disclosures of national defense information via her social media accounts.

On the day the article and book were published, Williams exchanged several messages with the Journalist. In one such message, Williams stated that she was "concerned about the amount of classified information being disclosed." In a separate message to a third party, Williams added that, "I might actually get arrested . . . for disclosing classified information." In a subsequent message, Williams citied a statutory provision of the Espionage Act.

And when asked how she knew that she may face legal consequences for her disclosures to the Journalist, Williams responded, "I have known my entire career," adding that "they tell you everyday . . . 100 times a day." Finally, in a message to a different third party, Williams stated that she was "probably going to jail for life." (Source)

Department of Veterans Affairs Employee Charged With Fraudulently Obtaining $73,000+ Of COVID-19 Benefits / Used Funds For Personal Expenses - April 10, 2026

Jesus Abreu, 38, who worked as a Food Service Worker with the Department of Veterans Affairs from November 2021 until March 2022, was indicted on three counts of wire fraud.

In July 2020, Abreu submitted an application for an Economic Injury Disaster Loan (EIDL) and received $32,400. In the application for the EIDL, Abreu made false claims regarding gross revenues. Subsequently, in April 2021, Abreu submitted two applications seeking Paycheck Protection Program (PPP) loans.

In those applications, Abreu allegedly made false claims regarding gross income purportedly earned from a sole proprietorship. To support these false claims, Abreu allegedly attached fraudulent tax documents as part of the applications. The PPP loan applications were approved and Abreu received $41,666. Abreu allegedly used that money on personal expenses. However, in September 2021, Abreu allegedly submitted loan forgiveness applications that falsely claimed the entire $41,666 was spent on payroll. Based on the misrepresentation the loans were forgiven. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

City Police Chief / City Administrator Sentenced To Prison For Stealing $307,000+ In City Funds - April 23, 2026

Daniel Paulino, 52, was appointed to the city administrator position in Velda City, Missouri in 2021. He was police chief until the department was dissolved in 2024, earning a salary of approximately $95,000 for the dual role. During an almost four-year period from 2021 to 2024, Paulino stole $307,100 in city funds. Paulino must repay $248,929 to the city, as some of the money was recovered.

Paulino Stole The City Funds In Various WayS

- Paulino caused three city checks totaling $1,800 to be fraudulently issued to him.
- Paulino caused about 20 direct deposits totaling $30,667 in city funds, purportedly for additional payroll, to be deposited into his personal bank account without the knowledge or approval of other city officials.
- On 17 occasions, Paulino used a city credit card to transfer a total of $37,500 in city funds to two businesses owned by Paulino and his spouse.
- He caused about 55 direct deposits of $54,693 in Velda City funds, purportedly for his spouse's payroll, to be sent to his personal bank account.
- Paulino used a city credit card, city checks and ACH transactions to pay for his personal expenses, including a $25,500 check for a 2007 International tow truck that he used in his private towing business.
- Paulino admitted using the money for travel, automobiles, pool supplies, utilities at his personal residence and food and beverage charges. (Source)

Healthcare Worker At USCBP Detention Facilities Pleads Guilty To $250,000 Fraud Scheme - April 23, 2026

Neery Velazquez admitted in federal court that while he was a healthcare worker (Contractor) at U.S. Customs and Border Protection detention facilities in San Diego County, he submitted almost $250,000 in false travel claims for reimbursement.

Contractor employees are eligible to request reimbursement of their lodging, meal and incidental expenses when they are on "Temporary Duty" (TDY) travel more than 50 miles from the employee's permanent home.

Velazquez was hired in January 2020 to work as a "traveler" performing contracted services for Customs and Border Protection (CBP) away from his permanent home in Las Vegas. In 2021, however, Velazquezt moved his permanent home to San Diego, making him ineligible for reimbursement for travel expenses.

Between 2021 and 2024, Velazquez submitted approximately 35 monthly travel claims to his employer and falsely attested that he was entitled to reimbursement of his lodging, meal, and incidental expenses because he was on TDY travel.

Velazquez also admitted he submitted forged documents to inflate and support his purported monthly expenses. This included a forged month-to-month lease agreement with a fake landlord, along with a forged rental receipt signed by the fake landlord, to make it appear as if he was paying thousands of dollars more for rent of a supposed temporary home each month than he was actually paying for his permanent residence.

In total, Velazquez submitted approximately $244,019.48 in false travel claims for reimbursement. CBP reimbursed approximately $181,082.85 of that amount before it discovered discrepancies in the submitted travel claims. (Source)

New York Corrections Officer Also Serving As A Navy Reservist Pleads Guilty To Fraudulently Obtaining $80,000 Of Military Leave Pay - April 9, 2026

Leah Mathieu, a correction officer with the New York City Department of Correction (DOC) and a Sailor in the United States Navy Reserve and New York Naval Militia, pled guilty to defrauding the DOC by falsely claiming tens of thousands of dollars in military leave pay.

Mathieu repeatedly made false representations and provided forged documentation, including purported military orders, to the DOC falsely claiming that she was on state active duty with the New York Naval Militia and therefore entitled to leave from her employment with the DOC.

Based on Mathieu's false representations and forged documentation Mathieu fraudulently obtained military leave pay from the DOC from December 2022 through March 2024, totaling approximately $80,297.90. (Source)

County Corrections Officer Pleads Guilty To $44,000 COVID Unemployment Loan Fraud Scheme - April 2, 2026

Jasmine Murphy had been a Corrections Officer with the Suffolk County Sherriff's Department from approximately January 2022 to December 2024. Prior to her employment with the Suffolk Sheriff's Department, Murphy fraudulently applied for pandemic unemployment and small business loan benefits while working for trucking and workforce services companies. While working at the Sheriff's Department, Murphy fraudulently collected UI benefits for a brief period of time early in her tenure. In total, Murphy obtained approximately $44,346 in unemployment benefits and small business loan funds to which she was not entitled. (Source)

U.S. Coast Guard Petty Officer Charged With Stealing $32,000+ For Fraudulently Applying For Temporary Lodging Allowance Funds - April 16, 2026

Mario Guzmán, an active-duty Petty Officer Second Class Maritime Enforcement Specialist in the United States Coast Guard (USCG) was arrested on April 1, 2026, for making a series of fraudulent Temporary Lodging Allowance claims and unlawfully receiving payments he was not entitled to receive.

According to the charges, on four separate occasions, Guzmán fraudulently claimed to the USCG, when applying for Temporary Lodging Allowance funds, that he and his family incurred reimbursable expenses by residing at a location called "Tony's Place," when in fact Guzmán and his family did not reside at Tony's Place, or incur in the claimed expenses. By making the fraudulent claims, Guzmán illegally stole approximately $32,260.00 in USCG housing allowance funds that he was not entitled to receive. (Source)

Dallas Police Department Sergeant Sentenced To Prison For Stealing Service Weapons & Selling To Pawn Shop - April 24, 2026

Thomas Fry, who at the time was a sergeant with the Dallas Police Department, admitted to three separate instances of taking a firearm owned by the Dallas Police Department, knowing that the firearms were stolen, and selling them to an Oklahoma pawn shop in June and July of 2022. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former City of Fresno California Art Council Manager Pleads Guilty To Embezzling $1.8 Million+ Of Publicly Funds / Used Funds For Gambling, Etc. - April 20, 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 began embezzling funds by making unauthorized withdrawals of money from the Fresno Arts Council's bank accounts. In 2023, after the Fresno City Council designated the Fresno Arts Council to administer the Measure P grant money, Caldwell significantly increased the amount of money she withdrew from the Council's accounts. Measure P is a tax initiative approved by Fresno voters in 2018 to provide funding for parks, trails, and the arts, among other things. In August 2023, the Fresno Arts Council received $9.4 million in Measure P funds, and in October 2024, it received an additional $5.7 million in a second round of funding.

Caldwell concealed the fraud by using her position of trust as the operations manager to alter and falsify financial reports that showed incorrect funds in Fresno Arts Council bank accounts. She presented these reports to the Fresno Arts Council executive director, board members, and others as accurate when they were not.

Between June 2022 and February 2026, Caldwell stole more than $1.8 million from the Fresno Arts Council. She then used the funds to gamble at local casinos, pay for vacations, and for other improper personal expenses. (Source)

Pennsylvania State Labor Department Employee Charged With Accepting Bribes To Approve $528,000+ In Fraudulent Unemployment Compensation Claims - April 21, 2026

From around June 2020, to around February 2023, Elizabeth Goss, 43, while working at the Pennsylvania Department of Labor and Industry, accepted unauthorized payments from unemployment compensation claimants to approve and expedite Pandemic Unemployment Assistance and other pandemic-related unemployment claims even though the claimants were not entitled to those benefits.

Goss's actions resulted in the payment of approximately $528,449 in unemployment compensation benefits to which claimants were not entitled. (Source)

State Government Librarian / Public Aid Eligibility Assistant Sentenced To Prison For Embezzling $102,000+ / Used Funds To Pay For Personal Vehicle Repairs - April 28, 2026

Kenyada Harris, 42, is the former director of the East St. Louis Public Library in Illinois. Harris admitted to embezzling more than $100,000 from the East St. Louis Public Library and the Illinois Department of Human Services.

Between March 2022 and March 2023, Harris was employed as a Public Aid Eligibility Assistant at the St. Clair County Family Community Resource Center through the Illinois Department of Human Services (IDHS). Harris was responsible for replacing lost, stolen, or damaged LINK cards and issuing new LINK cards to low-income IDHS customers to use to obtain food and cash assistance benefits. Instead of providing new customers with a LINK card, Harris would use the cards for herself, her family members and friends. Over the course of her scheme, records report that Harris used 98 distinct cards for her own personal gain. In total, her actions resulted in loss of over $10,000 to IDHS.

Around March 2023, Harris began working at the East St. Louis City Library as the Library Director. From July 31, 2023 through June 6, 2024, Harris knowingly used the Library's credit card to make personal purchases, including to pay for her personal vehicle repairs and to obtain cash advances. Harris' actions resulted in a loss amount to the East St. Louis Public Library in the amount of $91,937.

The judge also ordered Harris to pay $102,249 in restitution. (Source)

County Social Services Employee Sentenced To Prison For Stealing $100,000+ From Supplemental Nutrition Assistance Program / Used Funds For Personal Use - August 27, 2026

Shermeca McCrary, a Wayne County North Carolina woman, was sentenced to 6 months in prison, followed by 3 years of supervised release. She was ordered to to pay a Forfeiture Money Judgment of $102,000 for her role in a scheme to steal more than $100,000 in Supplemental Nutrition Assistance Program (SNAP) benefits administered by the United States Department of Agriculture and managed by the North Carolina Department of Health and Human Services, and county Division of Social Services. McCray unlawfully accessed the SNAP accounts of qualified individuals and stole $102,000 in government funds to her own personal benefit and use. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Los Angeles School District Employee Facing Charges For Role In $22 Million Contracts Kickback Scheme - March 27, 2027

A former Los Angeles Unified School District (LAUSD) IT employee and a tech company owner are facing felony charges in what prosecutors describe as one of the "largest" alleged money laundering schemes in the district's history.

Hong "Grace" Peng, a former LAUSD technical project manager, and Gautham Sampath, owner of the tech firm Innive, are accused of orchestrating a years-long "pay-to-play" scheme that allegedly steered more than $22 million in school district contracts to Sampath's company. Peng resigned from LAUSD in late 2022 after investigators executed search warrants at her home and workplace.

Peng played a role in awarding contracts tied to LAUSD's My Integrated Student Information System (MiSiS) between 2018 and 2022.

Authorities allege those contracts totaling $22 million were largely directed to Innive. Investigators say Sampath then funneled more than $3 million back to Peng through intermediaries. Prosecutors say messages between the two show discussions about deleting chats, securing contracts and moving money.

Peng, a Pasadena resident, was charged with felony counts of money laundering and illegally holding a financial interest in government contracts. Sampath faces similar charges, along with an additional count of aiding and abetting a public official. (Source)

Private School Bookkeeper Sentenced To Prison For Embezzling $1 Million+ / Used Funds For Credit Card & Mortgage Payments - April 9, 2026

Alysa Gisser, 56, was employed as a bookkeeper and accountant for a non-profit private school in Austin for children with special needs and learning disabilities. Beginning in or around 2018, she began embezzling money from the school, directing parents to make tuition and other payments to a PayPal account connected to her consulting business.

Gisser had renamed her business PayPal account to reflect the name of the school to misdirect the school's funds.

Additionally, she modified the school's accounting files to reflect that funds had been paid to the school, when in reality the funds had been transferred to her personal bank account to make credit card and mortgage payments, and install an in-ground swimming pool at her residence.

In total, between the PayPal payments and the checks deposited into her personal bank account, Gisser embezzled more than $1 million from the school. She also underreported her income by $863,963.32 between 2018 and 2021. (Source)

Former Director Food Services For Public Schools Charged With Stealing $11,000 Of Food & Equipment For His Side Business - April 22, 2026

Patrick Van Cott, 64, was the former Director of Food Services for the Plymouth Public Schools in Massachusetts, from 2003 until June 2025. Starting in approximately 2014, he also operated a seasonal business called the "Snack Shack" on Sandy Neck Beach in Barnstable, Mass. he allegedly stole food and commercial kitchen equipment for use and sale at his private business

It is alleged that, between 2014 and June 2025, Van Cott defrauded the Plymouth Public Schools by taking food and equipment purchased with funds including U.S. Department of Agriculture (USDA) funds and using that food and equipment to run Snack Shack. The equipment Van Cott is alleged to have ordered with school funds includes two $2,200 refrigerators; a $3,950 two-door freezer; two 12-inch hot plates; a 24-inch griddle; a chargrill; a fryolator; shelving; a sandwich prep table; a convection oven; and hanging chalk boards. In addition, every summer starting in approximately 2014, Van Cott is alleged to have collected condiments, diced chicken, hot dogs, cooking oil, snacks, paper goods, coffee, food products and other miscellaneous items paid for by the Plymouth Public Schools or supplied by the USDA, which he then used and sold those items at Snack Shack. He is further alleged to have directed Plymouth Public Schools cafeteria workers to slice at least nine pounds of deli turkey and 4.5 pounds of deli ham, which he sold in various menu items at the Snack Shack, once or twice per week starting in 2014. Van Cott is also alleged to have ordered over $3,000 in premium burger patties with school funds, which he intended to and did sell in menu items at the Snack Shack. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS
No Incidents To Report

LABOR UNIONS
No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS
No Incidents To Report

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES
No Incidents To Report

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Tesla Suing Vendor Matthews International For Stealing $1 BILLION In Trade Secrets – March 11, 2026

Tesla Vice President Bonne Eggleston explained the latest updates in a trade secret theft case the company has against a former manufacturing equipment supplier, Matthews International. Back in 2024, Tesla had filed a lawsuit against Matthews International, alleging that the firm stole trade secrets about battery manufacturing and shared those details with some of Tesla's competitors.

The two companies' relationship began back in 2019, as Tesla hired Matthews to help build the equipment for its 4680 battery cell. Tesla shared confidential software, designs, and know-how under strict secrecy rules.

Fast forward a few years, and Tesla reportedly caught Matthews copying the tech into machines that were sold to competitors, claiming they lied about doing so for three years, and continued to ship it.

That is when Tesla chose to sue Matthews in July 2024 in Federal court, demanding over $1 billion in damages due to trade secret theft.

Now a Judge issued a permanent injunction banning Matthews from using certain stolen Tesla parts or designs in their machines. Matthews is also officially "liable" for damages. The exact amount would still to be calculated later.

Matthews hit back with a press release claiming victory. They say an arbitrator ruled they can keep selling their own DBE equipment to anyone and rejected Tesla's request for a total sales ban. They call Tesla's claims "nonsense" and insist their 20-year-old tech is independent. Both sides are spinning the same narrow ruling: Matthews can sell their version, but they're blocked from using Tesla's specific secrets. (Source)

Funeral Home Employee Sentenced To Prison For Fraudulently Obtaining $11,000+ Through Identity Theft Scheme - March 31, 2026

Ronald Woolfolk was employed as a licensed mortician apprentice at a funeral home in Fayette County, Kentucky/ In his position, Woolfolk had access to the personal identifying information of clients and deceased persons, as well as the funeral home's email address.

From August 2022, through October 2023, Woolfolk defrauded a charity that financially supported families affected by the tragedy of losing a child.

Using the funeral home's email address, Woolfolk submitted approximately 23 requests to the charity seeking financial assistance on behalf of both real and fictitious deceased persons and their families.

The requests contained false information and fictitious documentation to support the requests for funding, including fake invoices for funeral expenses, fake cremation certificates, and fabricated letters using the funeral home's letterhead. Woolfolk directed the payments to a fake company he created.

Of the approximately 23 fraudulent requests for assistance, Woolfolk sought assistance with funeral expenses for three real deceased babies/toddlers and two young adults. Neither the funeral home, nor the family members of the deceased, knew of Woolfolk's actions. In total, Woolfolk fraudulently obtained $11,929.49 from the charity. (Source)

Company Files Lawsuit Accusing Former Executive Of Stealing Rare Earth Trade Secrets Months Before Resigning, Then Started Working For Competitor - March 20, 2026

A federal trade secrets lawsuit filed n Wyoming accuses a former executive at one of the state's highest-profile mining operations of stealing confidential data and carrying it to a direct competitor in the fast-moving race for American rare earth dominance. Rare earth elements are the strategic minerals used to build everything from fighter jets to smartphones to electric vehicles. China currently controls the vast majority of global production.

The complaint, filed March 16, 2026 in U.S. District Court for the District of Wyoming, alleges that Alex Moyes who served as director of critical minerals and planning at Ramaco from January 2024 to October 2025, emailed more than 40 sensitive technical and financial documents to his personal Gmail account in the months before resigning, then took a vice president position at rival USA Rare Earth Inc.

Ramaco filed the lawsuit alongside an emergency motion for a temporary restraining order, seeking immediate court intervention before, as the company alleges, evidence can be destroyed.

A forensic investigation of Ramaco's computer systems uncovered what the company describes as a systematic pattern of "data theft" spanning Moyes' final three months on the job. (Source)

Facebook Employee Arrested & Under Investigation For Downloading 30,000 Private Facebook Photos - April 7, 2026

A former Meta employee suspected of downloading around 30,000 private images of Facebook users is being investigated by the Metropolitan Police. The engineer, who lives in London, is believed to have designed a program to be able to access personal pictures on the site while avoiding security checks.

A Meta spokesperson told the BBC the breach was discovered over a year ago, after which the firm said it immediately fired the suspected employee and "referred the matter to law enforcement".

A spokesperson for the Metropolitan Police said a man in his 30s was arrested in November 2025 on suspicion of unauthorized access to computer material. He has since been released on bail, and must next report to police in May 2026. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

Discord Users Gained Unauthorized Access To Highly Sensitive Anthropic's AI Model Mythos / Anthropic's Vendor Had Privileged Access - April 22, 2026

An anonymous group of Discord users says it hacked its way into accessing Claude Mythos Preview, the new AI model Anthropic claims is too powerful for a public release.

Anthropic says Claude Mythos "is capable of identifying and then exploiting zero-day vulnerabilities in every major operating system and every major web browser," and has granted access to the model to a select of partners via an initiative called Project Glasswing. The AI company said this invite-only approach would let tech leaders "secure the world's most critical software."

As Bloomberg reports, the Discord users didn't gain access through a sophisticated hack, but by guessing the online location for the model based on past Anthropic naming conventions — as found in the recent data breach at Mercor, an AI startup, earlier this month.

Once they identified where to access Claude Mythos, the group had to employ additional tactics.

One member of the group already had privileged access as a worker at a third-party contractor for Anthropic, Bloomberg reports.The group was part of a private Discord channel that focuses on hunting information about unreleased models.

A member of the group told Bloomberg that they were not using Claude Mythos for nefarious purposes, but for tasks like building simple websites. However, they also claimed to have access to even more unreleased Anthropic models.

The group provided enough evidence to convince Bloomberg they had indeed breached Anthropic's security. Anthropic confirmed in a statement to Bloomberg it was aware of the claim and investigating.

At this time, there is no indication that Claude Mythos has been breached by other unauthorized parties. (Source)

Legal Protections Not Valid When Employees Post Trade Secrets Into AI Systems

Every time an employee pastes proprietary source code, a customer list, or a confidential business strategy into ChatGPT, Claude, or Google Gemini, they may be quietly dismantling the legal protections that make those secrets worth protecting. Courts and regulators are only beginning to grapple with this problem, and right now, the burden of preventing it falls squarely on employers.

Under the federal Defend Trade Secrets Act (DTSA) and the Uniform Trade Secrets Act (UTSA) as adopted across most states, a trade secret plaintiff must show that the information at issue was subject to reasonable measures to maintain its secrecy.

Courts have historically credited measures like confidentiality agreements, physical access controls, and employee training—but those safeguards were designed for a world of thumb drives and disgruntled employees. They were not built for a world where a well-meaning engineer can, in seconds, transmit an entire corpus of proprietary data to a third-party AI platform operating under terms of service that may permit the provider to use inputs for model training.

The trade secret implications are direct. Just as a privilege holder cannot claim confidentiality over communications routed through a third party with independent access rights, a company that inputs trade secrets into a public AI tool—particularly one that cannot guarantee confidentiality—risks a finding that it voluntarily

disclosed that information to an outside party. That finding would be fatal to the reasonable measures element of any subsequent trade secret claim. (Source)

Report States That Gen Z Workers Are Sabotaging AI Systems For Fear Of Job Replacement - April 8, 2026

Nearly half of Gen Z employees admit to actively undermining their employers' AI strategies, according to Writer's 2026 "AI Adoption in the Enterprise" report, released this week in partnership with Workplace Intelligence. The survey of 2,400 knowledge workers across the U.S., U.K., and Europe revealed that 29% of all employees have sabotaged their company's AI efforts in some way — jumping to 44% among Gen Z. The top reason? Fear of job replacement, cited by 30% of those confessing to the tactic.

Sabotage isn't subtle. Workers report feeding proprietary data into unapproved public AI tools, refusing sanctioned platforms, producing intentionally shoddy outputs, or even manipulating performance metrics to make AI look ineffective. No wonder 76% of executives see employee pushback as a major threat to their AI ambitions.

This revolt brews amid skyrocketing demands on young talent. A fresh SAP and Wakefield Research study of 100 U.S. CHROs shows 88% believe AI is fast-tracking early-career hires to role readiness. Seventy-nine percent hand enterprise AI tools to newbies within their first month, and 87% expect instant proficiency.

Governance lags. Fifty-six percent of CHROs note juniors default to rogue AI when guidance is fuzzy, while 44% flag uneven tool access as a top attrition driver for Gen Z, who feel perpetually one step behind.

Goldman Sachs economists peg AI at erasing 16,000 net U.S. jobs monthly, hitting entry-level roles hardest. Still, 60% of firms plan to axe AI resisters, even as 75% of C-suites admit their strategies are performative theater lacking real internal support. (Source)

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

U.S. Judge Fines Chinese Telecom Firm $50 Million For Stealing Trade Secrets From Motorola Worth $200 Million - March 20, 2026

Hytera Communications Corporation pleaded guilty to stealing trade secrets for walkie-talkies from Motorola Solutions. Motorola filed an appeal seeking restitution on top of a $50 million fine the judge ordered in the criminal case. Separately, Hytera is ordered to pay Motorola Solutions more than $400 million in a lawsuit.

Hytera has been fined $50 million by an Illinois federal judge for conspiring to steal trade secrets from Motorola. This decision follows the backdrop of an intensely fought legal battle that sheds light on the complexities of intellectual property theft within the tech industry.

The imposed fine comes alongside the roughly $600 million that Hytera has been directed to pay in a parallel civil case. The court determined that this civil payment offsets the amount required in the criminal matter, effectively countering the government’s push for an additional $290 million in restitution.

Motorola has filed an appeal saying the judge erred when he decided not to order Hytera to pay any restitution to Motorola Solutions in the criminal case — just the $50 million fine that goes to the government. Motorola Solutions said the “blatant theft of trade secrets” caused a loss of more than $200 million to the company.

Hytera was accused of recruiting Motorola employees in order to steal documents and computer source codes. One internal memo by Hytera spoke of the need to “defeat Motorola” in the walkie-talkie market.

In 2008, the Federal Communications Commission required radio manufacturers to transition from analog to digital walkie-talkies. Until the alleged Hytera thefts, the Chinese company was years behind Motorola in making that shift, prosecutors said.

Seven Hytera employees were also indicted in 2021 in federal court for their alleged roles in the thefts from Motorola. Gee Siong Kok pleaded guilty in 2022 to a federal charge of conspiracy to steal trade secrets. As part of his plea deal, Kok agreed to cooperate with the government and is awaiting sentencing. Arrest warrants have been issued for the six other defendants. (Source)

Aviation Company Employee Pleads Guilty To Attempting To Take Proprietary Information To China - April 1, 2026

In September 2019, Customs and Border Protection (CBP) stopped Junjie Zhang at an airport in Dallas, Texas, as he was attempting to board a flight to China. During an interview, agents asked if he had any work-related information on his electronic devices to which he responded, "no". Zhang told the agents the thumb drive and laptop he carried only contained personal information.

However, when CBP agents examined the devices, they discovered documents belonging to Zhang's employer marked "Proprietary" and "Confidential" along with graphs and blueprints associated with the aviation company's work. Zhang then changed his story to say that his employer had given him permission to have the documents.

CBP alerted the FBI who contacted Zhang's employer. The company informed the FBI that Zhang was not authorized to have confidential documents on his personal devices or to leave the country with that information. (Source)

2 U.S. Nationals Sentenced To Prison For Fraudulent U.S. Remote Information Technology Worker Scheme That Generated $5 Million In Revenue F Democratic People's Republic of Korea - April 15, 2026

The Justice Department today announced the sentencings of two U.S. nationals, Kejia Wang, 42, and Zhenxing Wang, 39, for their roles in facilitating North Korean (Democratic People's Republic of Korea (DPRK) remote information technology (IT) workers posing as U.S. residents to obtain work at more than 100 U.S. companies.

From approximately 2021 until October 2024, the defendants and their co-conspirators compromised the identities of more than 80 U.S. persons to obtain remote jobs at more than 100 U.S. companies, including many Fortune 500 companies, and caused U.S. victim companies to incur legal fees, computer network remediation

costs, and other damages of at least $3 million. Kejia Wang traveled to Shenyang and Dandong, China on two separate occasions in 2023, to meet with overseas actors about the scheme, including a former classmate that Kejia Wang knew was from North Korea. Kejia Wang went on to serve as the U.S.-based manager for the scheme, supervising at least five facilitators in the United States who collectively hosted hundreds of computers of U.S. victim companies at their residences. Zhenxing Wang was among the U.S. facilitators who received and hosted victim company laptops at his residence.

He and the others also enabled overseas IT workers to access the laptops remotely by, among other things, connecting the laptops to hardware devices designed to allow for remote access.

Kejia Wang and Zhenxing Wang created shell companies with corresponding financial accounts, including Hopana Tech LLC, Tony WKJ LLC, and Independent Lab LLC, to make it appear as though the overseas IT workers were affiliated with legitimate U.S. businesses.

In fact, these companies had no employees or operations and existed only to further the scheme and enable the defendants and their co-conspirators to receive proceeds from the scheme. The financial accounts established by the two defendants for these shell companies ultimately received millions of dollars from victimized U.S. companies, much of which was subsequently transferred to overseas co-conspirators. In exchange for their services, Kejia Wang, Zhenxing Wang, and the four other U.S. facilitators received nearly $700,000 for their respective roles in the scheme.

IT workers employed under this scheme also gained access to sensitive employer data and source code, including International Traffic in Arms Regulations (ITAR) data from a California-based defense contractor that develops artificial intelligence-powered equipment and technologies.

Specifically, between on or about January 19, 2024, and on or about April 2, 2024, an overseas co-conspirator remotely accessed without authorization the company's laptop and computer files containing technical data and other information. The stolen data included information marked as being controlled under the ITAR. (Source)

Married Couple Convicted Of Stealing Trade Secrets From U.S. Pediatric Research Institution Where They Worked, Loose U.S. Citizenship / Ordered To Pay $2.6 Million In Restitution - April 10, 2026

A married couple from China, who were convicted of stealing trade secrets from the US pediatric research institution where they worked, have now lost their naturalized US citizenship and face likely deportation back to China. The development comes amid indications from the Trump administration that it would prioritize denaturalization in cases related to economic espionage.

On March 30, 2026 a federal judge in California granted the US Department of Justice's (DOJ's) request that Li Chen and Yu Zhou be denaturalized, concluding that they had committed 'crimes involving moral turpitude' that prevented them from having the 'good moral character' necessary to naturalise.

In 2020, the pair admitted stealing a proprietary method for isolating exosomes – biomolecule-carrying vesicles that are released by many cell types – from samples of blood or other fluid. According to the DOJ, the pair conspired to monetise the technology by creating exosome 'isolation kits' that were to be sold by a company that Chen had set up in China. Exosomes are being researched for their potential in the identification and treatment of various medical conditions.

Chen and Zhou worked in separate medical research labs at NCH for a decade, overlapping for nine of those years, and received funding from the Chinese government's Thousand Talents programme, according to the DOJ.

After having completed prison sentences of 30 and 33 months, respectively, Chen and Zhou were serving three years of supervised release when their citizenships were revoked. The two have been ordered to pay $2.6 million (£1.96 million) in restitution to NCH and Chen also had to forfeit approximately $1.4 million in company stocks. The US government has indicated it may continue to seize their assets, regardless of whether they are in the US or back in China. (Source)

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

No Incidents To Report

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

20 Year Employee Pleads Guilty To Embezzling $3.7 Million Use Various Fraud Schemes - April 20, 2026

Barry Anderson, 68, was a 20-plus year employee with a multinational company specializing in industrial explosives and technical and blasting services, who served in various roles throughout the years.

In his role as regional president, Anderson embezzled approximately $400,000 through a fraudulent invoice scheme. Anderson coordinated with Gregory Shuey, the owner of a backhoe and dump truck business, to falsify 373 invoices from 2016 to 2023. Anderson directed the business owner either to greatly inflate the invoices or create fake invoices for services that were never performed. Anderson then paid these invoices on behalf of his employer to Shuey's business. Shuey then deposited the checks into a bank account that he controlled. From there, he gave Anderson a 50 percent cut of the fraudulently obtained funds as part of their arrangement. Anderson's employer paid approximately $2,432,844 in fraudulent invoices to Shuey's business.

In addition to Anderson's fraudulent invoice scheme, he also caused his employer to make lease payments to himself and others under false and fraudulent pretenses. Anderson and his confederates created limited liability companies (LLC)s which they owned and controlled.

Through the LLCs, they purchased properties which they then leased to Anderson's employer. Anderson caused his employer to enter into lease agreements under false pretenses by concealing the fact that he and his confederates were benefitting financially from the deals. From 2014 to 2023, Anderson was linked to 34 invoices seeking rental payments from his employer, totaling approximately $954,330. (Source)

Chief Financial Officer Sentenced Prison For $4.5 Million Fraud Scheme - April 9, 2026

In March 2022 Jonathan Leissler was hired as the chief financial officer for an industrial supply company in Warrensville Heights, Ohio. In this role, he was entrusted to manage payroll, expenditures, accounts payable, and company credit cards. However, in his first month on the job—and despite already receiving a six-figure salary—he created fake payroll records to add unauthorized extra money to his paychecks in the form of bonuses, commissions, and other payments. Investigators determined that by November 2024 he stole $3.8 million across 70 pay periods.

While Leissler continued to add unauthorized payments to his paychecks, he was also using the company's credit cards to make donations to his own election campaign in his bid for a seat on the Ohio Senate during the November 2024 general election. He utilized an online fundraising platform to collect more than $700,000—charged on the company's credit cards—toward his failed election campaign. When his employer confronted him about the credit card charges, Leissler processed refunds from the fundraising platform. However, the online platform was left on the hook for refund amounts because he had already changed the bank connected to the account to a different one that did not exist.

Another source of funds Leissler accessed was through a local Fraternal Order of Police (FOP) organization. While serving as their treasurer, he was issued a debit card and checkbook for the FOP account, which he then used to write checks to himself, withdraw cash, and pay his personal credit card bills. Ultimately, he stole more than $50,000 from the FOP on 69 separate occasions. The amount accounted for 80% of the organization's funds which had been earmarked to provide scholarships for the children of police officers. (Source)

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

Employee Pleads Guilty To Embezzling $26 Million+ From Employer With Help Of Boyfriend / Used Funds To Pay Off Vehicles, Living Expenses, Credit Cards, Etc. - April 24, 2026

Cynthia Marabella admitted that, from January 1, 2018, to about February 28, 2025, she and her boyfriend co-defendant William Costa devised a scheme to defraud Marabella's employer. 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 pay off vehicles, living expenses, and credit cards. They also purchased high-end merchandise with the stolen funds, such as expensive purses, shoes, clothing, and jewelry. Marabella sold the merchandise through an online consignment company. Marabella and Costa received more than $245,000 from the sales. As a result of the fraud scheme, Marabella and Costa obtained more than $26 million from the employer. (Source)

Accounting Department Manager Charged For Embezzling $3.9 Million Over 13 Years / Used Funds For Travel, Clothing, Entertainment - April 28, 2026

Colleen Kieran, 57, oversaw the accounting department of a business based in Seminole County Florida.

Over the course of nearly 13 years, Kieran used her position to siphon more than $3.9 million from the company's accounts into her own personal PayPal account. After taking the money, Kieran spent it on clothing, travel, entertainment, dining, consumer electronics, and entertainment media. Throughout the scheme, Kieran obtained loans in the company's name to conceal the stolen money. She also provided false information about the company's finances to her employers and the company's tax preparer. (Source)

Company Account Manager Sentenced Prison For Embezzling $2.8 Million+ / Used Funds For Luxury Items, Credits Cars & Real Estate - April 2, 2026

From December 2017 to July 2023, Tae Jones, 50, was an account manager for her employer in Garden Grove in California. In this role, her responsibilities included administering the company's accounting and financial operations. She had access to and control of the company's financial systems, corporate accounts, and records and had check-signing authorities on the company's bank accounts.

Without her employer's knowledge or consent, Jones transferred company funds from her employer's corporate accounts to her personal bank accounts to finance personal expenses. To conceal her scheme, Jones falsified her employer's account records to hide her unauthorized takings of company money. She used the mail to send and deposit company check into her various accounts.

For example, in July 2023, Jones mailed a $42,600 check from her employer's bank account to American Express, to be applied to her own credit card balance. To deceive her employer, Jones falsely represented this payment in her employer's records as a payment to a company vendor for material costs.

In total, Jones defrauded her employer out of approximately $2,894,441 in funds. She used the funds for home mortgages, jewelry, car loans, and personal credit card charges. (Source)

Chief Financial Officer Convicted Of Embezzling $1 Million+ Over 5 Year / Used Funds For Luxury Furniture, Designer Apparel, Etc. - April 20, 2026.

Tina Feuerstein, 53, served as the Chief Financial Officer of a Pennsylvania company that was owned by a company in the Chicago area.

Feuerstein used a company credit card over the course of five years to purchase personal items, including luxury furniture, designer apparel, and everyday expenses. To conceal her theft, Feuerstein falsified entries in the company's general ledgers to offset the amounts that she had stolen. She also deleted items in the company's expense-reporting system to hide more than 3,800 credit card charges that she had made totaling more than $1 million.

In addition, Feuerstein prepared false consolidated financial statements misstating the company's total expenses that her employer relied upon to make business decisions. The evidence at trial also showed that Feuerstein had previously embezzled more than $250,000 while working in the accounting department of another company. (Source)

Company Accountant Sentenced To Prison For Role In Stealing $393,000+ From Her Employer / Used Funds For Personal Use - April 22, 2026

Laura Dudley, 45, was employed by a Washington, D.C.-based nonprofit organization that provided educational programs, training, and development assistance in the Middle East and North Africa. She joined the organization in January 2008, initially as an administrative assistant responsible for purchasing supplies on a corporate credit card. She later transferred to the Accounts Receivable Department as an accountant.

Dudley stole more than $393,340 from her nonprofit employer by making unauthorized personal purchases on the organization's corporate credit card.

Beginning on or about January 1, 2020, Dudley and co-conspirator Daniel Park began using the organization's corporate credit card to purchase items on Amazon.

They bought gift cards, electronics, and beauty products for their personal use. Dudley and Park had the packages shipped to both the organization's headquarters and their personal residences. The organization paid the credit card bill each month.

Employees were required to log all credit card purchases and upload supporting invoices into an electronic expense system. To conceal the scheme, Dudley and Park failed to report their unauthorized purchases and, in some instances, Park created fake invoices that were uploaded into the log to cover the personal transactions.

The scheme was facilitated in part by the COVID-19 pandemic, during which Park was among the few employees working in person at the organization's headquarters, enabling him to receive Amazon packages on Dudley's behalf. Dudley also came into the office periodically to pick up her deliveries.

The fraud was discovered when the organization's new Chief Financial Officer questioned the volume of Amazon purchases in the Administration Department. Law enforcement subsequently uncovered Dudley's participation and determined that she had received about $333,825 of the about $393,340 stolen from the organization. She was terminated by the organization on May 3, 2022. (Source)

Arrest Warrant Issued For Home Owners Association Property Manager Who Stole Hundreds Of Thousands Of Dollars From HOA's / Used Funds For Plastic Surgery - April 8, 2026

A South Florida property manager is accused of siphoning off hundreds of thousands from local HOA accounts, then allegedly blowing the cash on plastic surgery, vacations and shopping sprees before vanishing, according to police.

The Martin County Sheriff's Office said it has obtained an arrest warrant for Alexandra Gonzalez, 46, in connection with an investigation into alleged fraud involving HOA accounts she managed while employed by Avant-Garde Property Management.

Gonzalez faces two counts of fraud exceeding $50,000, two counts of grand theft, 61 counts of uttering false instruments and 59 counts of embezzlement, according to the sheriff's office. Her total bond has been set at $1.35 million.

Investigators allege Gonzalez wrote checks to herself from HOA accounts over an extended period and concealed the thefts by creating fictitious invoices and false ledger entries. Authorities also say she forged the signatures of authorized account holders. (Source)

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Employee Sentenced To Prison For Embezzling $3.8 Million Over 8 Years Using Altered & Fake Invoices Causing Company Serious Harm - April 15, 2026

Bridget Thebeau was sentenced to prison for embezzling $3.8 million from her employer with the help of co-conspirators in China.

Thebeau struck a deal with some of her employer's suppliers in China to inflate purchase orders in exchange for kickbacks. She altered some purchase orders and issued others that were fictitious.

Between 2015 and 2023, she altered 152 purchase orders and issued 82 completely fictitious purchase orders, for a total of $3.82 million. In return, her co-conspirators wired more than half of that money to her personal bank account.

Assistant U.S. Attorney Justin Ladendorf wrote in a sentencing memo. Thebeau did not have a drug problem, financial issues or mental health problems that might have motivated her to steal from her employer. Judge Clark characterized Thebeau's embezzlement scheme as one of the worst he's seen during his time on the bench.

Thebeau tried to hide her crime with fraudulent shipping labels and fraudulent bills of lading issued by the China-based suppliers, fraudulent invoices that she created and claimed she had issued to the company's customers and false information she supplied to the company's owner and accountants. When her embezzlement was discovered, she deleted records from the company's server, submerged her laptop in a sink full of water, tried to destroy evidence on her cell phone and deleted information that was stored in the cloud, according to testimony in Monday's hearing. The owner of Thebeau's former company is no longer able to retire and has been forced to sell. (Source)

Chief Operating Officer For Art Museum Charged With Embezzling $ 600,000+ Using Fraudulent Invoices Scheme / Used Funds For Personal Benefit - April 14, 2026

The former chief operating officer of the High Museum of Art in Georgia, was arraigned on federal charge of theft concerning programs receiving federal funds. Lum allegedly used his position at the High Museum to steal more than $600,000 from the museum by doctoring invoices and approving transactions for personal purchases.

During his tenure as COO, Brady Lum repeatedly purchased non-business items and services for himself, including luxury guitars and other music equipment, personal music lessons, and woodworking equipment, through direct supplier invoicing and through the High Museum's corporate credit card reimbursement process. Lum concealed the nature of his transactions in several ways, including by submitting altered invoices, using his position to exercise delegated expense approval authority, and using accounting adjustments to spread his expenses across different cost centers so that they would not be readily identified.

For example, in one instance, on or about November 29, 2024, Lum submitted an altered invoice for reimbursement through the High Museum's online expense processing platform. While the submitted invoice showed a $9,147.87 purchase of equipment that appeared to be for the museum's benefit, the original version of the invoice was for a guitar and accessories. Over the course of his scheme, Lum stole more than $600,000 from the High Museum. (Source)

Employee Sentenced To Prison For Embezzling $478,000 By Submitting Fraudulent Invoices For Payment - April 6, 2026

Between June 2017 and December 2020, Miles Elletson knowingly and fraudulently devised a scheme to defraud Business-1 of approximately $478,013.

To fraudulently obtain money, Elletson entered false entries on work orders and submitted fraudulent invoices claiming that Advanced Purchasing Services LLC (APS) performed work for Business-1, when Elletson knew that was not true. That caused Business-1 to issue checks to APS for the fraudulent invoices, checks that Elletson often signed on behalf of Business-1. Elletson provided the checks to the registered owner of APS who deposited the checks. Elletson then instructed that individual to write checks from the APS account to other accounts, fraudulently claiming he used the specified accounts to buy the supplies APS sold to Business-1. In actuality, the accounts were Elletson's personal accounts, and the charges on the accounts were personal expenses. (Source)

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

Employee Pleads Guilty To Hacking & Sabotaging His Employers Network, Then Extorting Employees For $750,000 To Stop Attack - April 2, 2026

Daniel Rhyne, 59, worked as a core infrastructure engineer at a U.S.-based industrial company headquartered in New Jersey (Victim-1).

Around November 2023, Rhyne took steps to execute a scheme to hack Victim-1's computer network and extort Victim-1 into paying a ransom. Rhyne initiated unauthorized remote desktop sessions and prepared for the attack by scheduling tasks that would trigger damage to Victim-1's network. These tasks included deleting network administrator accounts, changing passwords to certain other Victim-1 accounts, and shutting down multiple Victim-1 servers. On November 25, 2023, Rhyne began deploying the scheduled tasks and, on the same date, sent an extortion email to Victim-1 employees in which he threatened to continue shutting down Victim-1 servers unless and until he received approximately 20 bitcoin, which, at the time, was valued at approximately $750,000. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Former New Jersey Transit Employee Pleads Guilty To Stealing 1000 Phones & Selling Them Making $900,000 / Used Funds For Travel - March 31, 2026

A former New Jersey (NJ) Transit supervisor pleaded guilty to stealing more than 1,000 cell phones from the agency and reselling them, a scheme that netted him almost a million dollars over the course of about four years.

37-year-old Peejay Manila began the theft in November 2020. Manila would purchase cell phones intended for NJ Transit employees, but instead sold many of the phones to buyback companies and used the money for travel, including to Japan and Dubai. He was working as the chief of NJ Transit's digital workspace when he committed the theft. Manila will be tasked with repaying the approximately $1,383,000 lost by NJ Transit. He made about $900,000 from the scheme. (Source)

Computer Systems Administrator For Federal Public Defender's Office Charged With Stealing & Selling Government Property - April 2, 2026

Peterson Bernadel was a Computer Systems Administrator (CSA) at the Office of the Federal Public Defender for the District of Connecticut (FDO). As a CSA, he had physical access to the FDO's inventory of digital and electronic devices, including computers, tablet computers, cellular telephones, and other devices. He also had the ability to add, remove, and edit information contained in their digital inventory record-keeping system.

Brendel stole property from the FDO, including iPads, Apple and Dell computers, a Mavic drone, and a Canon digital camera, and exchanged the items for cash at pawn shops. He also falsified an inventory record related to an Apple laptop computer that he had stolen and pawned. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

No Incidents To Report

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

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

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

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)

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

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 the National Insider Threat Special Interest Group (NITSIG), and after reviewing NITSIG Monthly Insider Threat Incidents Reports.

WHO CAN BE AN INSIDER THREAT?

- ☐ 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)

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

There are many different types of Insider Threat incidents 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 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, OpenAI, 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

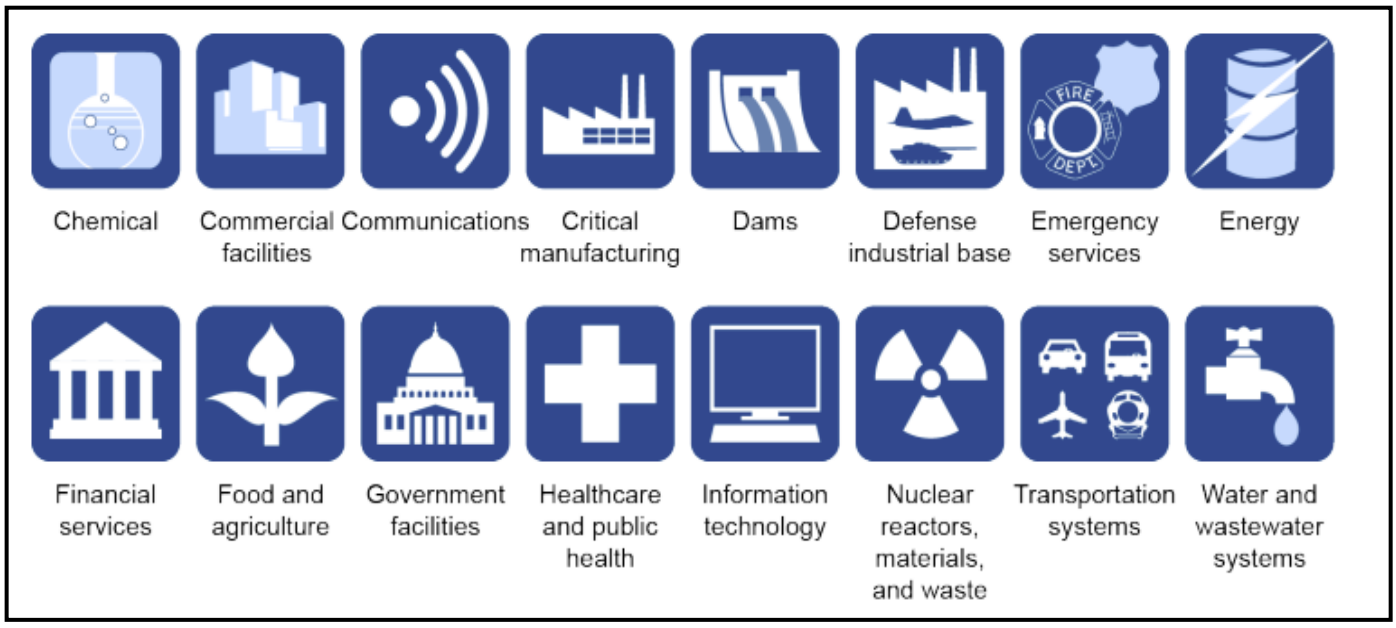
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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 2024 REPORT ON FRAUD

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

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

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

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

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

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

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

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

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

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

Fraud In Government Organization's / Infographic

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

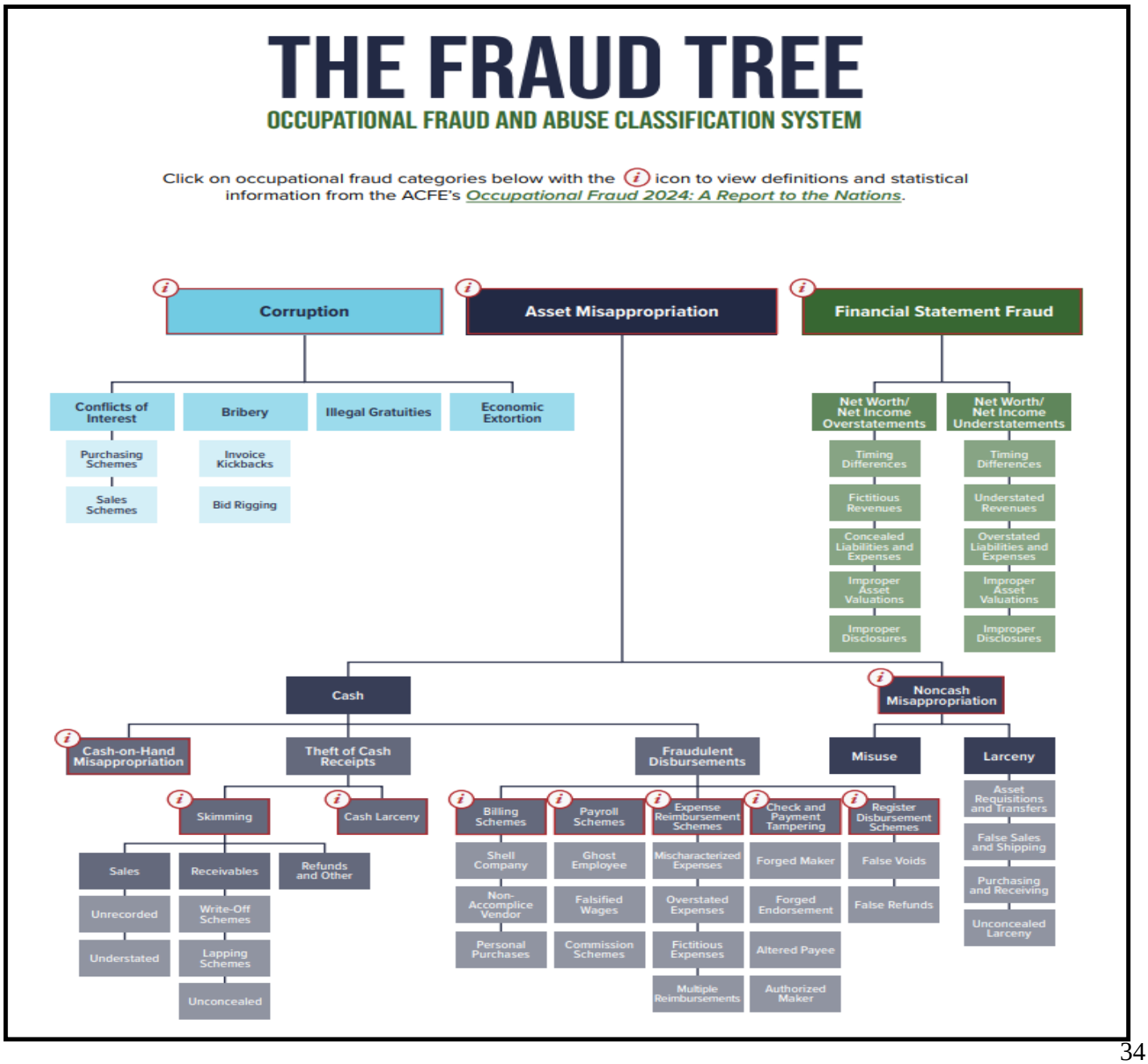
Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators



SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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 (**7,000+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS 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)

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)

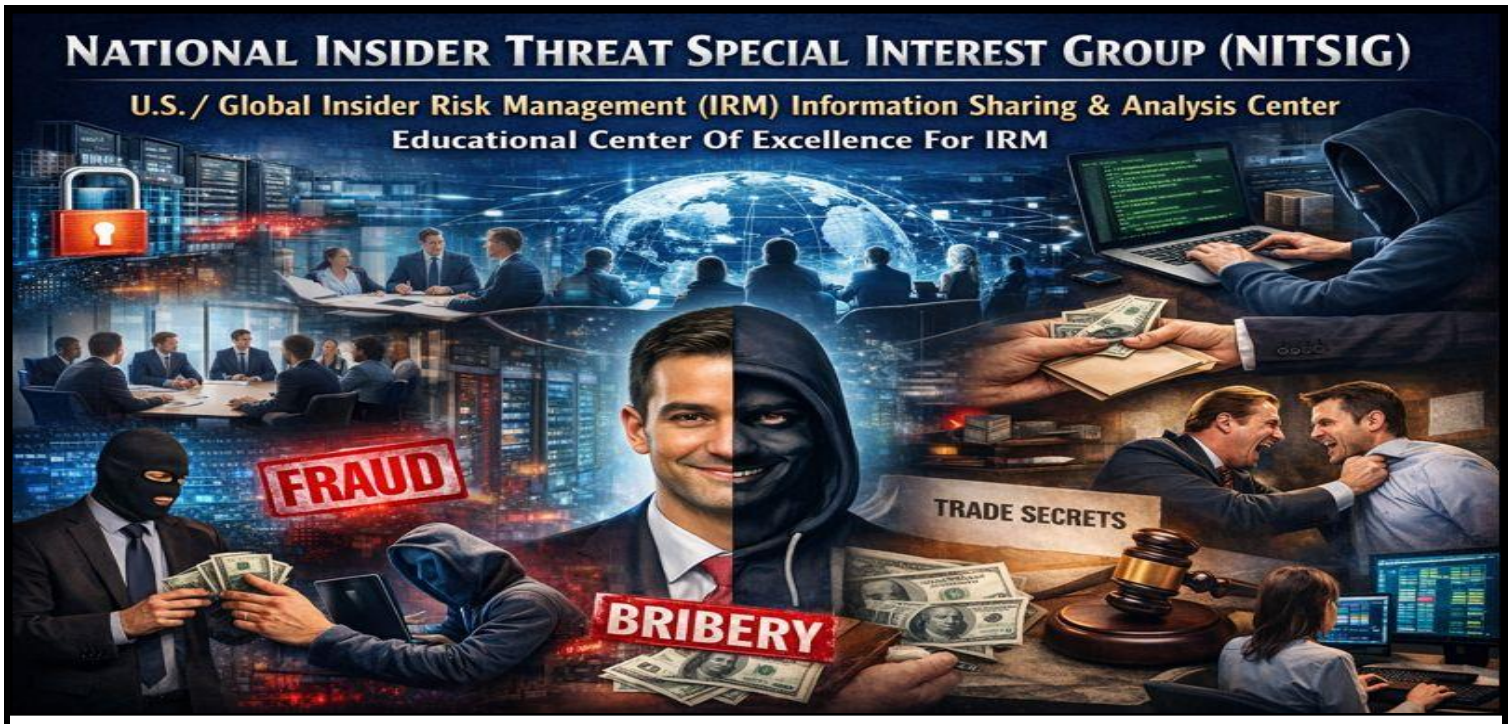
Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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, as no such ISAC existed. The NITSIG has been successful in bringing together Insider Risk Management (IRM) and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats. Many members have even stated the NITSIG is like having a team of IRM experts 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)
- ✓ Insider Threat Investigations & Analysis
- ✓ IRM Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Employee Continuous Monitoring & Reporting Programs (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 website are various documents, resources and training that will assist organizations with their IRM / IRM Program efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with over 900 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: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

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

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
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 Insider Risk Management (IRM) Programs (IRMP's).

The ITDG exceeds IRM compliance regulations and help organizations create comprehensive, robust and 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 Training Course & Workshops For C-Suite, Board Of Directors, Insider Risk Program Manager / Working Group Members
- ✓ IRMP Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees

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 IRM Consulting Services For Our Clients

STUDENT / CLIENT SATISFACTION

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, due to the fact that the ITDG approaches IRM from a real world, practical, strategic, operational and tactical perspective. 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. 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 Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG