INSIDER THREAT INCIDENTS REPORT FOR

October 2026



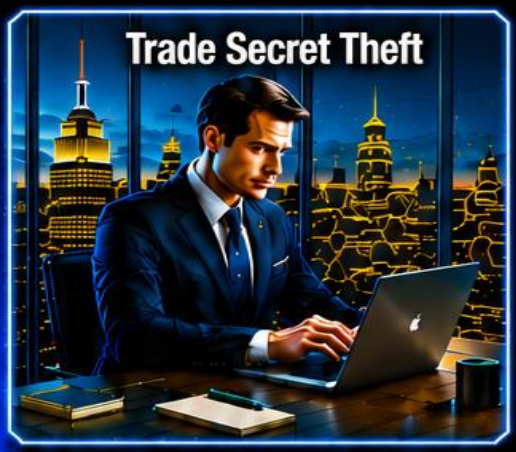








DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM









Produced By

National Insider Threat Special Interest Group

Insider Threat Defense Group

TABLE OF CONTENTS

	PAGE
Insider Threat Incidents Report Overview …….	3
Insider Threat Incidents For October 2026 ……	4
Insider Threats Definitions / Types ……..	28
Insider Threat Impacts, Damaging Actions / Concerning Behaviors ……...	29
Types Of Organizations Impacted ……	30
Insider Threat Motivations Overview ……..	31
What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations ……	32
2026 Association Of Certified Fraud Examiners Report On Fraud …….	33
Fraud Resources ……	39
Severe Impacts From Insider Threat Incidents …….. Billion Dollar Impacts / Company Goes Out Of Business	40
Insider Threat Incidents Involving Chinese Talent Plans …….	62
Other NITSIG Insider Threat Specialized Reports ……	64
National Insider Threat Special Interest Group Overview ……	67
Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview ……	69

INSIDER THREAT INCIDENTS OVERVIEW

A Very Costly And Damaging Problem

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees' who are negligent, malicious or opportunists. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **7,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

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

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

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

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

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

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

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report and others will show. **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 25** 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 OCTOBER 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

UAE's Attorney General States That Flydubai Co-Pilot Attempted To Carry Out A Premeditated Terrorist Act By Assaulting The Captain -October 4, 2026

The UAE's Attorney General recently confirmed that the Flydubai Flight FZ1073 co-pilot, 29-year-old Omani national Hamam Al Hammami, attempted to carry out a premeditated terrorist act by assaulting the captain with the cockpit's own emergency crash axe in an attempt to crash the plane into Israel's Ben Gurion Airport.

The incident, which took place on September 30, 2026, while the Boeing 737 MAX 8 was over Saudi Arabia with 174 passengers and eight crew members aboard, resulted in a terrifying 14,000 to 17,000-foot plunge in less than a minute before control was regained.

Hammam is a Omani national who was previously suspended from flying by Oman Air after being identified as a security risk, according to senior intelligence and law enforcement officials.

Officials investigating the incident are still trying to determine how the suspected attacker was subsequently permitted to fly for FlyDubai and how he ended up as the first officer in the cockpit of a plane headed for Israel, the sources said.

Hammami appears to have operated an account on X (formerly Twitter). A review of over 3,000 archived posts from the now-deleted account in 2021 and 2022 pointed to intense religious conservatism and misogyny, including approving references to violence against women. (Source)

Australian Institute Of Insider Threats - Insider Threat Incidents Weekly Reports

https://www.insiderthreats.au/threat-warning

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES

No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS

No Incidents To Report

U.S. GOVERNMENT

2 U.S. Postal Workers Sentenced To Prison For Stealing & Selling $84 Million Worth of U.S. Treasury Checks - October 19, 2026

4 individuals have been sentenced to prison: Saahir Irby, 28, Tauheed Tucker, 25, Cory Scott, 26, and Alexander Telewoda, 26

Between June 2023 and September 2024, Irby and Tucker, while working as United States Postal Service (USPS) mail processing clerks, stole thousands of envelopes containing U.S. Treasury checks from mail sorting machines at the USPS Philadelphia Processing and Distribution Center.

Irby and Tucker removed the checks from the USPS facility and sold them to defendants Scott and Telewoda, who then advertised the stolen checks for resale on the Telegram app.

Upon receiving payment from interested buyers, Scott and Telewoda mailed the stolen Treasury checks to buyers around the country who attempted to cash the stolen checks.

Over the course of the scheme, Irby and Tucker sold Scott and Telewoda thousands of stolen Treasury checks whose face value exceeded $84 million. Scott's and Telewoda's customers successfully negotiated approximately $11 million worth of these stolen Treasury checks at financial institutions. (Source)

U.S. Postal Service Employee Sentenced To Prison For Role In Stealing $34 Million Worth Of Checks From Mail - October 9, 2026

Destinee Ruffin, 29, of Indianapolis, has pleaded guilty to orchestrating a $34 million conspiracy to commit bank fraud by stealing checks from the U.S. Mail. 3 of Ruffin's co-conspirators have already been sentenced for their roles in the scheme. One additional co-conspirator, John Young, is awaiting a sentencing date.

Ruffin was employed as a letter carrier at the Bacon Station Post Office in Indiana. Between November 2020 and May 2022, Ruffin used access to both incoming and outgoing mail to steal checks, which he then sold to co-conspirators.

In April 2024, officers executed a search warrant on Ruffin's vehicle, residence, person, and electronic devices. They discovered thousands of stolen checks valued at over $20 million that Ruffin had stolen but not yet sold. (Source)

U.S. Postal Service Employee Charged With Stealing $55,000+ Of Money Orders - October 15, 2026

Kyree Hall, 26, was an employee of the U.S. Postal Service in 2025, and worked as the sole clerk in the Rio Oso Post Office in Sutter County.

Using his position, between March and May 2025, Hall issued at least 56 USPS money orders payable to himself and falsely recorded that they had been paid for by various people. The theft cost the U.S. Postal Service approximately $55,505. (Source)

U.S. Postal Service Employee Sentenced To Prison For Submitting $166,000+ Of Fraudulent Unemployment Insurance Claims - October 15, 2026

Christopher Powell, 37, worked as a letter carrier with the USPS and previously pleaded guilty to two counts of wire fraud. At the time of his guilty plea, Powell admitted that from July 2020 through January 2024, he submitted fraudulent unemployment insurance (UI) claims in multiple states using his own personal identifying information and made false certifications to obtain and maintain such benefits.

In July 2023, after spending the stolen benefits associated with one false claim, Powell falsely reported to his bank that he never received the UI funds, prompting the bank to issue him even more money he was not entitled to. The judge ordered Powell to pay restitution in the amount of $166,366.53. (Source)

U.S. Postal Worker Pleads Guilty To $20,000+ Fraudulent COVID-19 Loan - October 19, 2026

Court documents reflect that in 2021, Dominique Stanberry, 33, while working full time as a United States Postal Service employee, caused to be submitted a fraudulent online application for a PPP loan that falsely claimed she was self-employed with a business that lost income due to the COVID-19 pandemic. As a result of her fraud, the defendant received $20,833 in PPP loan funds to which she was not entitled. (Source)

United States Postal Service Employee Sentenced To Prison For Stealing $16,000+ - October 28, 2026

Merri Ann Bentley, 42, admitted that she stole over $16,000 from the United States Postal Service (USPS) in about 2023. Burgart made false entries in the USPS's travel mileage system in order to obtain reimbursements for fictitious mileage that she allegedly incurred while delivering mail on rural routes in a personal vehicle. For example, on August 19, 2023, Burgart falsely claimed reimbursement for 727 miles she had allegedly driven on Route 1 in the Waverly area, which was not true, and as a result she received mileage reimbursement to which she was not entitled. Burgart earned nearly $100,000 a year at the time she was stealing from the USPS. (Source)

U.S. Congressman Sentenced To Prison For Secretly Acting As Agent Of Venezuelan Government & Obtaining A $50 Million Contract- October 2, 2026

Former U.S. Congressman David Rivera was sentenced today to 10 years in federal prison for secretly acting as an unregistered agent of the Venezuelan government and laundering millions of dollars connected to that work.

Rivera and co-defendant Esther Nuhfer obtained a $50 million contract with a subsidiary of Venezuela's state-owned and state-controlled oil company, Petróleos de Venezuela, S.A. (PDVSA), to advance the interests of the Venezuelan regime in the U.S. Without registering as foreign agents as required by law, Rivera and Nuhfer lobbied U.S. officials, including then-U.S. Senator Marco Rubio and U.S. Representative Pete Sessions, and arranged meetings between U.S. policymakers and high-ranking Venezuelan officials, including then-President Nicolás Maduro and then-Foreign Minister Delcy Rodríguez. Rivera and Nuhfer used coded language in text messages to describe their activities.

The evidence at trial further showed that Rivera deposited approximately $1.5 million in proceeds from the contract to his Florida state congressional campaign account between March 2017 and August 2018, among other personnel uses. Nuhfer used approximately $455,000 in proceeds to purchase a residence in Key Colony Beach. (Source)

Department of Energy Employee Charged For Attempting To Provide Support To Terrorist Organization - October 1, 2026

Ashton Ellaboudy, 51, was arrested and charged with attempting to provide material support or resources to the Houthis, a designated foreign terrorist organization.

Ellaboudy, who was a Department of Energy employee, came to the attention of the FBI after they received information that he had purchased precursor chemicals, components, and other materials commonly used in the construction of homemade explosive devices. In addition to the precursor chemicals, the investigation revealed Ellaboudy had also purchased parts used for the construction of drones and remotely operated aerial systems.

In December 2024, the FBI learned that Ellaboudy took sick leave from his employment, claiming that it was due to having been exposed to highly concentrated nitric acid, a common chemical used in the construction of explosive materials. In September 2025, Ellaboudy, using an official passport previously issued to him when employed by the U.S. Army Corps of Engineers, traveled from Richland, Washington to Oman.

Upon arriving in Oman, Ellaboudy used this same passport to cross the border into Yemen with the intent on traveling to Sanaa, Yemen, the country's capital, which is under the control of the Houthis. Upon returning to the U.S., Ellaboudy stated to U.S. Customs and Border Protection Officers that he had travelled overseas on official government business. Subsequent information from Ellaboudy's DOE supervisor revealed he did not have any authorized official government travel to that region. (Source)

DEPARTMENT OF WAR / INTELLIGENCE COMMUNITY

Former CIA Officer Pleads Guilty To Creating Fabricated Special Access Program & Defrauding Federal Government Of Approximately $193 Million / Used Funds To Purchase Gold Bars Real Estate, Etc. - October 6, 2026

David Rush, 49, was employed in a senior executive-level position with a federal agency and held a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance. He reached that position, in part, by lying about his education and military experience.

Rush used his position of extraordinary public trust to create fictitious government authorities – including a fabricated Special Access Program – to obtain U.S. government funds for his personal benefit.

Once he received the funds, Rush acquired gold bars and directed approximately $145 million in wire transfers that he ultimately used to purchase luxury real estate, watches, and at least one car. As a result of his scheme, Rush fraudulently obtained approximately $193,590,400 in U.S. government funds.

On May 19, the FBI searched Rush's residence and recovered 298 gold bars, approximately $2,106,550 in cash and numerous luxury watches. Rush had obtained the gold bars at an approximate cost to the government of $46 million. Pursuant to the plea agreement, Rush has agreed to forfeit the gold bars and currency found at his home, the fraudulently obtained properties, 30 watches (many of which were Rolexes), and two 2026 BMW Alpina vehicles, at least one of which is valued at approximately $172,000. (Source)

U.S. Army Official Pleads Guilty To Accepting $55,000 In Bribes For Awarding Contracts - October 28, 2026

From January 2021 to October 2022, Carlos Duque conspired with two defense contractors, Brian Kent and Leonard Pick, to accept a bribe of approximately $1.25 million over five years. In return, Duque told prime contractors to award subcontracts to Kent and Pick's company and facilitated their fraudulent inflation of government contracting costs to include Duque's bribe payments. Duque ultimately received approximately $55,000 in bribes from his coconspirators and the United States Army paid over $3 million to Kent and Pick's company. (Source)

CIA Contractor Employee Arrested For Leaking Classified Information To Individual Who Posted On Substack - October 23, 2026

Following a referral from the Agency, on Friday, October 23rd, 2026 the FBI arrested a contractor (Ian Brinksman, 42) o who provided services to CIA for alleged unauthorized disclosures of classified information, said CIA Director John Ratcliffe.

Beginning in 2020, the contractor worked as an employee of the CIA and later in 2022 began working as a developer for systems integration for the CIA as a contractor, During all times relevant to the complaint, Brinksman held a Top Secret security clearance with Sensitive Compartmented Information (SCI) access.

Brinksman had an ongoing personal relationship with an individual who maintains an online publication on Substack. A fundraising article reportedly published in September 2026 claimed Brinksman had published reporting based on classified assessments. The individual posted the classified information on her Substack social media profile, claiming "I also accept leaks." (Source)

SECURITY CLEARANCE RELATED / WHISTLEBLOWERS

No Incidents To Report

CRITICAL INFRASTRUCTURE

Water Information Sharing & Analysis Center Insider Threats Report - October 8, 2026

This report finds that insider threats represent a growing and often underestimated risk to the water and wastewater sector, one that extends far beyond the popular image of a lone malicious employee sabotaging a facility for revenge. This report defines insider threat risk broadly as harm arising when trusted individuals—employees, contractors, vendors, or other authorized personnel—misuse or fail to protect the access they have been given, whether intentionally or unintentionally.

The authors contend that insider incidents are on the rise in virtual every sector, with unintentional or negligent insiders remaining the most frequent category while malicious insider incidents, the most financially and operationally damaging kind, are also increasing, driven in part by the rapid, often ungoverned adoption of AI tools that can amplify how quickly sensitive access is exploited.

In addition to AI, the report assesses that heightened geopolitical tensions, growing Information Technology (IT) and Operational Technology (OT) convergence, increased access by contractors and other third-parties to water and wastewater controls (including the use of remote access), and calls by violent extremists to recruit insiders in critical infrastructure organizations are together all heightening the risk of insider threats.

Moreover, the report examines five manifestations of insider risk specific to water and wastewater utilities, including unintentional errors, employee theft, cyber-enabled sabotage, disgruntled-employee retaliation, and workplace violence. Each real-world case study underscores how insider access can translate directly into public health, safety, financial, and reputational consequences.

Ultimately, the report argues that because insider threats are fundamentally a human problem rooted in behavior and organizational culture rather than technology alone, water and wastewater utilities must adopt a risk-informed, multidisciplinary approach spanning security, cybersecurity, HR, legal, and leadership to detect early warning signs and intervene before a concern becomes an incident. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S. Citizenship & Immigration Services Officer Sentenced To Prison For Accepting Bribes For 10 Years To Help Individuals With Immigration - October 1, 2026

Amara Dukuly,44, a former immigration officer employed by U.S. Citizenship and Immigration Services (USCIS), was sentenced today to 12 months and one day in prison, three years of supervised release, a $6,000 fine, and $6,000 in restitution for accepting a $6,000 bribe.

From approximately 2015 to 2025, Dukuly used his status as a USCIS employee to solicit bribes from individuals in exchange for promises to help them obtain assistance with their immigration status.

On April 4, 2025, Dukuly received a $6,000 bribe from an individual to help him with the removal of "terrorist" references from the individual's immigration file. Dukuly promised the individual that after the "terrorist" references were removed, his file would be "clean." (Source)

Assistant Superintendent For Norfolk County Sheriff's Office Sentenced to Prison For Ordering Employees To Perform Maintenance At His Home - October 26, 2026

Thomas Brady, 55, the former Assistant Superintendent at the Norfolk County Sheriff's Office (NCSO) was sentenced to prison for using his official position to order NCSO employees to perform maintenance at his residence. The defendant was also sentenced for witness tampering.

From 2021 through May 2023, Brady served as the Assistant Deputy Superintendent (ADS) for Jail Operations at NCSO. Brady was promoted in May 2023 to Assistant Superintendent.

In October and November 2022, Brady utilized his official position and authority as an ADS to order an NCSO maintenance officer (Maintenance Officer A), a subordinate in to Brady, to perform home repairs at his residence during and after work hours. , Maintenance Officer A feared that if he refused Brady's request to help fix his home heating system, Brady would use his official position and authority to negatively affect Maintenance Officer A's job position at NCSO including the possibility of causing Maintenance Officer A to lose his preferred shift schedule, position and/or employment at NCSO.

On June 16, 2023, another maintenance officer at NCSO, reported Brady to the Massachusetts State Ethics Commission (SEC) for having subordinate NCSO employees perform work at his private residence. The SEC subsequently initiated an investigation into Brady have maintenance officers do work at his home. (Source)

State Prison Correctional Lieutenant Pleads Guilty To Taking $95,000+ In Bribes To Smuggle Contraband Into Prison - October 20, 2026

Matthew Madsen, 40, was employed by the California Department of Corrections and Rehabilitation (CDCR) from 2017 to 2025. CDCR is a California State agency responsible for administering and operating the State's prison and parole system. Madsen was assigned to work at the Salinas Valley State Prison in Soledad, California, and held several ranks including Correctional Lieutenant. As a Correctional Lieutenant, Madsen often served as a supervisor for a whole yard of the prison – including approximately 1,000 inmates and 200 staff. CDCR employees are prohibited from bringing contraband, such as wireless communication devices and tobacco products, into state prisons.

Madsen admitted, wireless communication devices are particularly pernicious in prison because inmates can use them to coordinate violent attacks and the smuggling and trafficking of contraband. Nevertheless, from January 2023 through February 2025, Madsen worked with others, including at least one inmate and one individual outside the prison, to smuggle contraband into the prison in exchange for money. In total, Madsen received more than $95,000 for participating in the scheme, including cash payments and wire transfers. (Source)

LAW FIRMS

Law Firm Employee Sentenced To Prison For Stealing $173,000 - October 21, 2026

Sarah Steiner is a former employee of the Trey Morris Law Firm in Shreveport, Louisiana. She was sentenced to 10 years in prison for stealing roughly $173,000 from the firm and was ordered to pay $147,000 in restitution. The information released did not explain the $26,000 difference between the reported theft amount and the restitution order. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Virginia State Senator Indicted For Leading A Criminal Marijuana Distribution Enterprise Worth $4.5 Million - October 22, 2026

Virginia state senator Lillie Louise Lucas, 82, of Portsmouth, Virginia, led a criminal enterprise (the Lucas Enterprise) comprised of a close-knit group of associates and family members, including her two daughters and her grandson. Lucas allegedly approved and directed activities of the enterprise, including arranging for the acquisition and distribution of 100 kilograms or more of marijuana and supervising the laundering of marijuana proceeds.

Louise Lucas allegedly abused her position of public trust as a 30-year Virginia State Senator to put her own financial interests ahead of the people she represents, orchestrating a five-year scheme worth an estimated $4.5 million, said FBI Director Kash Patel. (Source)

2 City Employee Fired, 2 On Leave Following $14.7 Million Theft - October 26, 2026

One city employee has been fired and two others placed on paid administrative leave following an internal investigation into the theft of $14.7 million in taxpayer funds, Mayor Spiro Cheriogotis announced.

According to Cheriogotis, the theft was not an "inside job" or a technical system breach, but rather an elaborate vendor impersonation scheme that deceived key staff through fraudulent emails, documents, and phone calls. The city is withholding the employees' identities for safety reasons. The mayor said his administration will be working alongside the FBI and Secret Service to recover the funds and hold the perpetrators accountable. (Source)

South Carolina City Manager Employee Arrested For Embezzling $10,000+ Of City Funds - October 7, 2026

A former city of Union, South Carolina, employee has been arrested and charged with embezzling more than $10,000 in cash according to officials.

The South Carolina Law Enforcement Division said 65-year-old Kathy Teague is accused of embezzling the money from the city between January 2022 and June 2026. Teague was working as the manager for the building and zoning department during the time of the alleged embezzlement, SLED reports. (Source)

Contractor Employee For State Of Illinois Charged For Fraudulently Obtaining $4.6 Million+ In COVID Relief Benefits For Herself &100+ Others - October 19, 2026

Andrea Wellington is former employee of a State of Illinois subcontractor. She has been indicted on federal fraud charges for allegedly fraudulently obtaining more than $4.6 million in Covid-era unemployment insurance benefits for herself and hundreds of others. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School District Worker Accepted $70,000 In Kickbacks To Approve $156,000+ Of Fraudulent Overtime Sheets - October 23, 2026

A Pennsylvania man admitted to paying approximately $70,000 in cash kickbacks to former Hillsborough Township School District (HTSD) Business Administrator Aiman Mahmoud as part of a fraudulent overtime scheme undertaken by the two men in relation to a large-scale project involving the construction and upgrade of HTSD facilities.

Kenneth Gratto, 55, admitted that shortly after he was hired, he agreed to provide substantial cash kickbacks to Mahmoud in exchange for which Mahmoud approved Gratto's time sheets which substantially exaggerated the number of overtime hours Gratto worked and for which Gratto billed at a rate of $150 per hour. Specifically, Gratto admitted that he regularly submitted time sheets claiming that he had worked more than 12 hours of overtime work on both Saturdays and Sundays throughout the latter half of 2021 even though he had not performed any work on those weekend days.

After receiving his paychecks from the companies involved – who were in turn reimbursed by the HTSD for those amounts – Gratto would deposit the checks, withdraw cash in the amount of the intended kickback, and deliver that cash in an envelope at a location of Mahmoud's choosing, typically, within Mahmoud's unlocked school vehicle. Gratto admitted to paying Mahmoud approximately $70,000 in kickbacks generated from the fraudulently billed overtime hours.

In total, Gratto admitted to embezzling approximately $156,150.00 from the HTSD with Mahmoud via the overtime billing scheme. As part of his plea agreement with the Government, Gratto agreed to forfeit this amount. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

U.S. Citizenship & Immigration Services Officer Pleads Guilty To Stealing $60,000+ From Union - October 2, 2026

Carol Aguja, 55, is a former U.S. Citizenship & Immigration Services (USCIS) Officer. She pleaded guilty in federal court in Boston to stealing more than $60,000 from a labor union over the course of five years.

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

Between 2019 and 2024, Aguja defrauded AFGE Local 38 by siphoning funds from the union bank account to pay for her own personal and non-union related expenses. As part of her fraud scheme, Aguja also paid union expenses out of her personal accounts and commingled union and personal funds to conceal her embezzlement.

Specifically, Aguja used the AFGE Local 38 credit card to pay approximately $12,508 for personal expenses such as restaurant meals, bills, clothing and dance lessons. She also made 128 cash withdrawals totaling over $23,700 from the AFGE Local 38 account, and transferred over $25,000 from the AFGE Local 38 account to her personal accounts.

Aguja falsified annual forms regarding the union finances that AFGE Local 38 was required to submit to the United States Department of Labor-Management Standards, in order to conceal her fraud. (Source)

BANKING / FINANCIAL INSTITUTIONS

TD Bank Employee Pleads Guilty To Accepting $8,000+ In Bribes To Launder $4.8 Million To Colombia - October 6, 2026

Gerardo Aquino, 40, accepted bribes and exploited his position as a bank employee to help launder illicit funds to Colombia. From April 2022 to November 2023, Aquino opened fraudulent accounts, issued hundreds of debit cards to co-conspirators, and unblocked debit cards that TD Bank had restricted due to potential fraud.

The bank accounts and debit cards were then used to funnel approximately $4.8 million out of the United States. As part of this scheme, Aquino opened 86 individual customer accounts using the same exact commercial address in Miami. Those accounts alone were used to launder over $3 million in illicit funds to Colombia. In exchange, Aquino received more than $8,000 in bribes — paid in cash and through a peer-to-peer digital payment network. (Source)

Bank Employee Sentenced To Prison For Stealing $126,000 From Elderly Customer With Dementia - October 9, 2026

Beginning in or about May 2023, Carlos Bras, 41, accessed the account of the 78-year-old victim, who resided in an assisted living facility and had a court-appointed conservator in Massachusetts. Bras admitted that he enabled online banking access to the victim's account; ordered checks sent to addresses he controlled; obtained a debit card for personal use; and conducted numerous unauthorized transactions, including transfers to accounts controlled by him and his family and multiple wire transfers to a bank account in Portugal.

Investigators also discovered a purported real estate contract in Portugal bearing the signatures of Bras and the victim. The victim's conservator reported that the victim was unaware of the transaction and that the signature and listed address were not the victim's. (Source)

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

Amtrak Employee Sentenced To Prison For Role In $11 Million Health Care Plan Fraud Kickback Scheme Involving 19 Employees - October 7, 2026

Devon Burt, 53, is a former Amtrak employee. He worked with health care providers to recruit Amtrak employees to participate in a health care fraud scheme through the offer of cash payments, in exchange for the employees allowing health care providers to use their patient and insurance information to submit false claims. The health care providers benefitted from the scheme by receiving payments from the Amtrak health care plan for services that were never provided or that were medically unnecessary. Burt received cash payments from providers in return for allowing the providers to use his personal and insurance information, and that of his dependents, to submit fraudulent claims. Burt received cash payments from providers in return for recruiting others to participate in the scheme.

In or around April 2022 through June 2022, Burt and another conspirator conspired to communicate extortionate threats to a health care provider who participated in the scheme.

Burt and his conspirator threatened the provider by interstate telephone calls and text messages, indicating that the provider would be injured if the provider did not pay the conspirator several thousand dollars.

The overall scheme targeting the Amtrak health care plan involved dozens of Amtrak employees and multiple health care providers, who paid hundreds of thousands of dollars in cash kickbacks to Amtrak employees over the course of the scheme. In total, the Amtrak health care plan paid over $11 million in fraudulent claims associated with providers connected to the scheme.

The Amtrak health care plan paid out approximately $959,072 for claims associated with Burt. The investigation has resulted in the prosecution of nineteen individuals, including Burt. All have pleaded guilty to conspiracy to commit health care fraud. (Source)

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

OpenAI Claims Former Employee Stole 100+ Trade Secrets Files & Joined Apple - October 14, 2026

OpenAI claims a former employee took more than 100 files related to its product plans before joining Apple. In a document filed OpenAI accuses the unnamed employee of sending this information to a personal account and then presenting it to Apple leadership, including the vice president of the company's operations in Asia.

The filing, reported earlier by Reuters, is tied to a legal battle between Apple and OpenAI over trade secrets, but this time, OpenAI is doing the accusing.

It alleges that the files in question contain images of at least one unreleased device, along with supplier information, engineering data, project files, standards for cosmetic finishes, and reports about the "coating and sealing of hardware components."

OpenAI also links Apple's new HomeView smart display and the range of other devices it revealed this week to the former employee's presentation. "That presentation appears to have happened months ago, and now, armed with that information, Apple is making a new push into AI-enabled products," OpenAI claims, while citing an article and a company announcement about Apple's new product releases. (Source)

Regional Sales Manager Being Sued For Secretly Operating His Own Company That Was A Director Competitor To His Employer, And Diverted $10 Million+ Of Contracts To His Business - October 1, 2026
Scott Lee Snider, employed by Echelon International LLC as a Regional Sales Manager, secretly operated Warrior Won Contracting LLC, a direct competitor, while employed by Echelon.

He diverted at least three procurement opportunities worth approximately $10.725 million from Echelon to Warrior Won by using Echelon's confidential information, trade secrets, and connections, and failed to disclose his outside business. (Source)

Abbott Laboratories Employee Being Sued For Stealing Trade Secrets, Just Before Resigning & Joining Competitor - September 20, 2026
Chad Amato, a former senior Abbott employee in Arizona, repeatedly transmitted Abbott's confidential business information to his personal email accounts while employed, diverted a recruiting opportunity to competitor Impulse, and after resigning on September 1, 2026, wiped data from his company-issued iPad despite Abbott's instructions not to delete data.

Abbott alleges Amato breached contractual and fiduciary obligations, retained and transmitted trade secrets, destroyed evidence, and joined Impulse in a role substantially overlapping his Abbott duties. (Source)

Director Of Sales Being Sued For Stealing Trade Secrets Before Resigning To Help Competitor Win Business - September 25, 2026
Scott Bertram is the former Director of Sales for Northern California at GalleherDuffy.

Betram allegedly misappropriated trade secrets including sales data, customer account information, pricing information, and display placement reports prior to his resignation on January 23, 2026, and before his last day on February 20, 2026. He provided this information to HF Design, which used it in concert with Tri-West to divert Galleher Duffy's customers and usurp Plaintiffs' Palacio product lines. (Source)

Employee Being Sued For Starting Competing Business While Still Employed By Employer & Stealing 37,000 Customer Records - October 11, 2026
Joshua Bishop, a long-term Account Manager at Atlantic Diamond Tools (ADT's), Inc. planned his departure for months while still employed, forming a competing business (Bishop & Son Enterprises LLC) and exporting the company's entire CRM database of 37,000 customer records after resignation by exploiting a security gap in the CRM system. (Source)

Aviation Company Accusing / Suing Competitor For Hiring Employee Who Stole Trade Secrets - October 3, 2026
When George Kivork departed Joby Aviation in July 2025 to join competitor Archer Aviation, his departure likely seemed routine—a business development professional moving to a rival in the high-stakes eVTOL market. Six months later, Joby filed suit in Santa Cruz Superior Court alleging that Archer had weaponized confidential information Kivork had extracted. By October 2026, the case had survived multiple dismissal motions and was proceeding through the federal docket.

Archer Aviation is accused by Joby Aviation of hiring away employee George Kivork, who allegedly transferred confidential Joby files to a personal email account before his departure and modified security permissions to retain access after leaving. Joby's forensics investigation uncovered dozens of files moved to personal email and hundreds with altered permissions, indicating deliberate exfiltration and post-departure access.

When Joby's forensic team examined Kivork's deactivated accounts and company-issued laptop, they found: 1) Dozens of files transferred to a personal email account before departure, 2) Hundreds of additional files with modified security permissions that allowed continued access after employment ended, 3) Trade secrets spanning multiple domains: aircraft specifications, operations, site analysis, partnership terms
and business strategy. (Source)

Alabama Port Authority Manager Charged For Trade Secret Theft - September 2, 2026

Daniel Joseph Gill, a former Alabama Port Authority manager, was charged with nine counts of computer tampering, seven counts of theft of trade secrets, and two counts of possession of a forged instrument after an internal investigation revealed he accessed confidential information about 379 fellow employees.

Gill allegedly used the port's computer system to obtain confidential data and manipulate the bidding process to steer contracts to certain companies. The investigation, conducted by the Port Authority Police Department and referred to the District Attorney's Office, resulted in Gill's arrest in September 2026; he pleaded not guilty and was released on bond." (Source)

Database Administrator Who Abruptly Resigned Is Being Sued For Stealing Trade Secrets & Launching Denial Of Service Attacks Against Former Employer - October 15, 2027

Thomas Wade, a former Database Administrator at Resensys, LLC, allegedly misappropriated trade secrets after abruptly leaving the company in late March 2026.

Wade took proprietary code, design files, and credentials, published some on his personal website and the Python Package Index, and launched denial-of-service attacks using his former credentials. (Source)

Former Product Marketing Manager Being Sued By Previous Employer For Stealing Trade Secrets Days Before Resignation & Joining Competitor - October 15, 2026

Transcarent, Inc. filed a complaint against former employee Erin Jones and her new employer Garner Health Technology, Inc., alleging that Jones downloaded at least twenty-five confidential files from Transcarent's secured SharePoint and OneDrive systems to a personal Apple device in the days before her resignation, then joined competitor Garner and likely used or disclosed the stolen trade secrets.

The complaint states that Transcarent conducted a forensic investigation that uncovered the downloads on September 14, 21, and 22, 2026, and that Jones failed to return the files as required by her confidentiality agreement. (Source)

Account Manager Being Sued For Stealing Trade Secrets The Day Before Resigning To Join Competitor - October 20, 2026

Sean McKinstry, a former Account Manager at BrightView Landscapes, emailed a proprietary Bid Doc Estimator file containing confidential pricing formulas to his personal Gmail account on May 7, 2026, the day before resigning to join competitor Green Earth LLC. (Source)

Hewlett Packard Vice President Being Sued For Stealing Trade Secrets To Start Competing Business - October 22, 2026

Brian Wheeler, a former HPE Vice President, allegedly misappropriated HPE trade secrets by developing the 'Hero' AI tool using HPE resources and confidential data, then publishing it publicly under an alias while planning to leave HPE to start a competing business. Wheeler transferred HPE files to personal devices. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

The AI Incident Database is dedicated to indexing the collective history of harms or near harms realized in the real world by the deployment of artificial intelligence systems. AI Incident Database

Other AI Inicdents Tracking Websites

https://airisk.mit.edu/ai-incident-tracker
https://airisk.mit.edu/navigator#/incidents/browse
https://oecd.ai/en/incidents
https://aiincidenttracker.com/
https://aiincidents.org/explorer/
https://www.firetail.ai/ai-breach-tracker
https://fail.ticker.io/
https://www.pointguardai.com/ai-security-incident-tracker

South Korean Police Officer Arrested For 400+ AI-Generated Sexual Exploitation Videos & Sharing On Internet - October 4, 2026

A South Korean police officer was arrested for creating and distributing AI-generated fake nude videos of acquaintances and possessing thousands of illegal sexual exploitation materials. The officer used AI apps to fabricate over 400 fake videos and shared them via Telegram, continuing the crimes even after joining the police force. (Source)

Johns Hopkins Medical Center Employee Caused Patient Data Breach By Using Unauthorized AI Tool - October 25, 2026

An employee at Johns Hopkins Bayview Medical Center mistakenly uploaded a spreadsheet containing sensitive health information for 3,182 patients to an unnamed unauthorized third-party AI tool in late September. The spreadsheet included patient providers, admission dates, treatment, medications, and medical record numbers, but no social security numbers or financial information. The breach was discovered during an internal review. Johns Hopkins requested the AI tool's parent company delete the data, reinforced policies around approved tools, and began notifying affected patients in early October, offering 12 months of complimentary credit monitoring." (Source)

Wisconsin U.S. Rep. Derrick Van Orden Reportedly Posted Deepfakes Depicting Opponent Rebecca Cooke Saying Things She Did Not Say - October 1, 2026

Wisconsin U.S. Rep. Derrick Van Orden repeatedly posted Grok Imagine-generated videos depicting Democratic challenger Rebecca Cooke saying statements she did not make. Cooke called the clips deceptive and defamatory; Van Orden's campaign described them as obvious AI-generated satire.

In one such video, an AI-generated version of Cooke says “Let the peasants eat cake. They will vote for me anyway.” In another fake video, Cooke’s avatar says “There is a 100 percent chance I just voted for two Communists.” Cooke's attorneys later sent a cease-and-desist alleging the videos were intended to mislead voters and harm her reputation. (Source)

Oklahoma Judge Admitted To Using ChatGPT To Generate Fictitious Case Citations For Child Custody Case - September 11, 2026

A Stephens County judge admitted to state investigators he cited at least two cases in a court order that do not exist. Cases he says he found through ChatGPT.

The incident goes back to November, when Stephens County District Judge Lawrence Wheeler was overseeing a child custody case.

Wheeler denied a request from one of the parents' attorneys to have the other parent undergo a psychological test—and in his order denying the request, he pointed to multiple previous Oklahoma cases he said backed him up. The cases were not real. (Source)

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

14 Individuals Charged In North Korean Fraudulent Remote IT Workers Scheme Affecting 70+ U.S. Companies - October 13, 2026

The U.S. Attorney's Office for the Northern District of Ohio has announced the unsealing of a 58-page indictment charging U.S. citizens and Chinese nationals for their roles in an IT worker conspiracy affecting more than 70 U.S. companies. These charges are the result of a year-long investigation.

The defendants conspired to participate in a multi-year fraudulent scheme to obtain remote IT work to generate revenue for the government of the Democratic People's Republic of Korea (DPRK), which is more commonly referred to as North Korea.

The scheme was allegedly carried out by facilitators in the United States who assisted others working on behalf of the DPRK to be hired as remote IT workers with U.S. companies.

Among the ways used to carry out the scheme, U.S. facilitators received and hosted multiple laptop computers—issued by victim U.S. companies—at their residences in the U.S., referred to as "laptop farms."

In total, the scheme impacted more than 70 U.S. company employers and generated approximately $3 million in revenue for IT workers. The revenue is believed to have been sent to sanctioned entities controlled by the DPRK.

Victim entities included companies serving a broad array of industries and services including health care, communications, cyber support, retail, and manufacturing companies. Victim businesses were located not only in Ohio, but also across much of the U.S. including in Massachusetts, California, New York, New Jersey, Florida, Georgia, Minnesota, Maryland, North Carolina, Illinois, Virginia, Michigan, Texas, Arkansas, Pennsylvania, Washington, and the District of Columbia. (Source)

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

No Incidents To Report

INSIDER TRADING / STOCK TRADING & SECURITIES FRAUD

No Incidents To Report

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

No Incidents To Report

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

Chief Financial Officer Being Sued For Embezzling $5 Million By Manipulating Financial Documentation / Used Funds For Gambling & His Own Company - September 17, 2026

Derek Utley, former Chairman and CFO of X Strategies, embezzled at least $5 million from the company between 2021 and 2026 by disguising personal withdrawals as business expenses, gambling with company funds, diverting funds to his own entities (Stark Industries & Dicenzo Fitness), fabricating financial records, and taking unauthorized salary payments. The fraud was uncovered after a new president initiated a forensic audit that revealed suspicious transactions and led to Utley's admission of theft. (Source)

Business Accounting & Operations Manager Pleads Guilty To Embezzling $3.9 Million / Used Funds Clothing, Travel, Etc. - October 8, 2026

Colleen Kieran, 57, worked for a business in Seminole County, Florida where she oversaw accounting and operations. Beginning in 2009, Kieran abused her access to the company's financial accounts to divert customer payments to her personal accounts without authorization. Over time, the theft escalated to thousands of transfers, ultimately totaling more than $3.9 million. Kieran used the stolen money for personal expenses, including clothing, travel, dining, entertainment, and consumer electronics.

To conceal the scheme and the growing financial loss to the company, Kieran prepared false financial statements and spreadsheets and withheld information from the company's owners and tax preparer.

As the shortfalls grew, Kieran also obtained more than $1.5 million in loans in the company's name, without the owners' knowledge, to mask the missing revenue and keep cash flow appearing stable.

After the fraud was uncovered and Kieran was fired, her employers discovered that she had also been intercepting the company's incoming mail and that several years' worth of emails from her company account had been selectively deleted. (Source)

Company Chief Financial Officer Sentenced To Prison For Embezzling $1 Million+ / Used For Personal Items, Luxury Furniture, Designer Apparel, Etc. - October 28, 2026

The former Chief Financial Officer (CFO) of a Chicago-area company's subsidiary has been sentenced to three years in federal prison for embezzling more than $1 million.

Tina Feuestein served as the CFO of York Wallcoverings, a Pennsylvania company that was owned by a company in the Chicago area. Shortly after she was hired in 2016, Feuerstein began using a company credit card to purchase personal items, including luxury furniture, designer apparel, and everyday expenses. Over the next five years, Feuerstein falsified entries in the company's ledgers and deleted items in its expense-reporting system to hide more than 3,800 credit card charges totaling more than $1 million. Prior to working at York Wallcoverings, Feuerstein embezzled more than $200,000 while working in the accounting department of another company. (Source)

Human Resources Manager Sentenced To Prison For Stealing $1 Million+ / Used Funds For Gambling - October 7, 2026

For approximately two years between 2023 and 2025, Tahnya Shafer, 48, stole from her employer using multiple fraudulent schemes, including inflating her paychecks and causing apparently legitimate payments to vendors to be sent to her bank accounts instead of the vendors. In total, the Defendant stole over one million dollars, the vast majority of which she spent at casinos in North Idaho. As a result, the employer fell behind on bills, and the owners had to tap their own funds to keep their employees paid.

The ordered that Shafer be placed on supervised release for three years following completion of her prison sentence. Shafer was also ordered to pay $1,040,126.27 in restitution to her former employer. (Source)

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

Director Of Food Services For Public School Systems Sentenced To Prison For Stealing $11,000 Of Food & Equipment For His Food Side Business - October 7, 2026

Patrick Van Cott, 64 was the Director of Food Services for the Plymouth Public Schools from 2003 until June 2025. Beginning in 2014, he also operated a seasonal business, the "Snack Shack," on Sandy Neck Beach.

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 it to run the Snack Shack.

The equipment Van Cott ordered with school funds included 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 chalk boards. In addition, every summer beginning in approximately 2014, Van Cott 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, then used and sold those items at the Snack Shack. Additionally, once or twice per week every summer starting in 2014, Van Cott directed Plymouth Public Schools cafeteria workers to slice at least nine pounds of deli turkey and 4.5 pounds of deli ham which he then sold at the Snack Shack. Van Cott also 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)

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Commercial Real Estate Employee Pleads Guilty To Embezzling $1 Million From Employer By Creating Fraudulent Invoices - October 14, 2026

Christopher Septon, 52, pleaded guilty to one count of wire fraud and embezzlement of more than $1 million from his former employer.

From 2019 until 2024, Septonn devised and executed a scheme to defraud and embezzle from his former employer, Ellis Properties, a small family-run business in Minneapolis that specializes in commercial real estate. Septon worked for Ellis Properties and was trusted to use company funds to pay vendors, contractors, and other third parties.

Septon abused his position to improperly charge more than $800,000 on the company credit card, directing the payments to his own payment-processing accounts. He wrote false statements in the transaction memo lines, misrepresenting to the company that the transactions were business-related and with third parties, when in fact they were transfers to his own accounts. He then transferred the fraud proceeds to bank accounts he controlled.

Septon created fake invoices, emails, and lies to induce Ellis Properties personnel to issue him reimbursement checks for expenses he did not actually incur.

To fraudulently induce payments, the defendant also falsely represented that various payments pertained to work with various third parties, including government agencies, such as the City of Minneapolis, the Metropolitan Council, the Minnesota Department of Agriculture, and the Minnesota Pollution Control Agency. (Source)

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

No Incidents To Report

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

Engineer Working For Industrial Company Sentenced To Prison For Network Sabotage & $750,000 Extortion Scheme Of His Employer - October 5, 2026

Daniel Rhyne, 59, worked as a core infrastructure engineer at a U.S.-based industrial company headquartered in New Jersey. In November 2023, Rhyne took steps to execute a scheme to attack his employer's computer network and his extort his company into paying a ransom. Rhyne initiated unauthorized remote desktop sessions and prepared for the attack by scheduling tasks that would trigger damage to his employer's network.

These tasks included deleting network administrator accounts, changing passwords of other accounts, and shutting down multiple servers.

On November 25, 2023, Rhyne sent an extortion email to employees in which he threatened to continue shutting down servers unless and until he received approximately 20 bitcoin, which, at the time, was valued at approximately $750,000.

Forensic investigators found that on November 22, Rhyne used a hidden virtual machine and his account to search the web for information on clearing Windows logs, changing domain user passwords, and deleting domain accounts as he planned his extortion plot. One week earlier, Rhyne made similar web searches on his laptop, including "command line to remotely change local administrator password" and "command line to change local administrator password." (Source)

Terminated Employee Steals Proprietary Pricing Data For 1,100 Customers / Login Credentials Were Not Deactivated - September 21, 2026

A.W.G. Dewar, Inc., a tuition refund insurance specialist, alleges a former account executive accessed its Constant Contact customer database on April 22, 2026 five days after being terminated on April 17, 2026.

The employee exported contact details, decision-maker information, and proprietary pricing data for approximately 1,100 school customers (representing roughly 33 years of average client relationships each). The employee's Constant Contact login credentials were not deactivated during the termination process, despite access restrictions normally limiting the system to three senior staff members.

According to the federal complaint filed September 17, 2026, the ex-employee subsequently joined Vertical Insure (a competitor in the niche tuition refund market) as School Partnerships & Growth Lead and began soliciting Dewar customers using the exported data. Dewar values the misappropriated trade secrets at over $1 million and alleges the breach caused considerable competitive harm." (Source)

Senior Engineer Being Sued For Stealing His Employers Source Code On Last Day Of Employment, Then Deleting Original Copy - October 10, 2026

John Arens, a Senior FPGA Engineer at Geneva Trading USA, LLC, copied the entire FPGA source code repository to a personal USB drive labeled on his last day of employment (June 30, 2026) and deleted local copies to conceal the act. The theft was discovered later via an enhanced security review of Geneva's FPGA work system. (Source)

EMPLOYEE WHO INSTALL COVERT ELECTRONIC DEVICES IN THEIR EMPLOYERS OFFICIES

OpenAI Employee Arrested For Installing Audio Recording Device At OpenAI Office In San Francisco - October 13, 2026

An employee of OpenAI, an artificial intelligence, company headquartered in San Francisco, has been arrested for and charged with using or endeavoring to use an electronic, mechanical, or other device to intercept oral communications. Abdulrahman Alfozan, 35, a national of the Kingdom of Saudi Arabia, was arrested on Friday, October 9, 2026.

Alfozan had been employed as an engineer by OpenAI since July 2025. On or about September 30, 2026, OpenAI personnel discovered a surreptitious audio recording device inserted into a USB port on the back of a television in an executive conference room inside one of OpenAI's buildings in San Francisco. OpenAI determined that the device, which had been concealed in toilet paper, was installed on or about September 28, 2026, and that its contents were encrypted.

Closed-circuit television (CCTV) footage inside OpenAI's office showed that Alfozan appeared near the executive conference room on multiple dates prior to the device's discovery, although he had no authority to access, or to participate in meetings occurring in, the executive conference room. According to the complaint, meetings in the executive conference room where Recording Device 1 was discovered frequently involved discussions of highly confidential technical, commercial, and strategic information, including proprietary research, product plans, and business-development opportunities, as well as nonpublic information about OpenAI's technical progress and strategic decisions, capabilities, priorities, government engagements, and commercial relationships. (Source)

NOTE

Sometimes the simplest of threats are overlooked. Has your organization checked computers, servers, tv's for electronic devices that can record audio and video, and also checked computers and servers for usb keylogger devices?

THEFT OF ORGANIZATIONS ASSESTS / DESTRUCTION OF PROPERTY

No Incidents To Report

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

Skechers Tennis Shoe Executives Being Sued For BILLON DOLLAR Fraud To Drive Down Stocks Before Selling Company - October 22, 2026

A proposed class of shareholders sued the popular shoe brand Skechers, claiming the company collaborated with a private equity firm and a financial adviser to artificially drive down stock value ahead of last year's shareholder buyout.

The plaintiff, SM Merger /Arbitrage L.P., a private investment fund, accuses Skechers leaders of orchestrating a multibillion-dollar fraud scheme with private equity giant 3G Capital, which purchased the company last year, and financial adviser Greenhill & Co., which aided in the negotiations.

The proposed class action, filed Wednesday in the Central District of California, stems from Skechers' September 2025 sale to 3G Capital, which took the publicly traded shoe company private. The private equity firm bought the company for $9.4 billion. The plaintiff says the defendants disseminated false and misleading statements, omitted facts and manipulated financial projections to deflate the company's stock price and facilitate a more lucrative deal. (Source)

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

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

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
www.insiderthreatincidents.com



INSIDER THREATS DEFINITION / TYPES

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

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

INSIDER THREAT (Simplistic)

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

INSIDER THREAT (Expanded)

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

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

Other Damaging Impacts To An Employer From An Insider Threat Incident

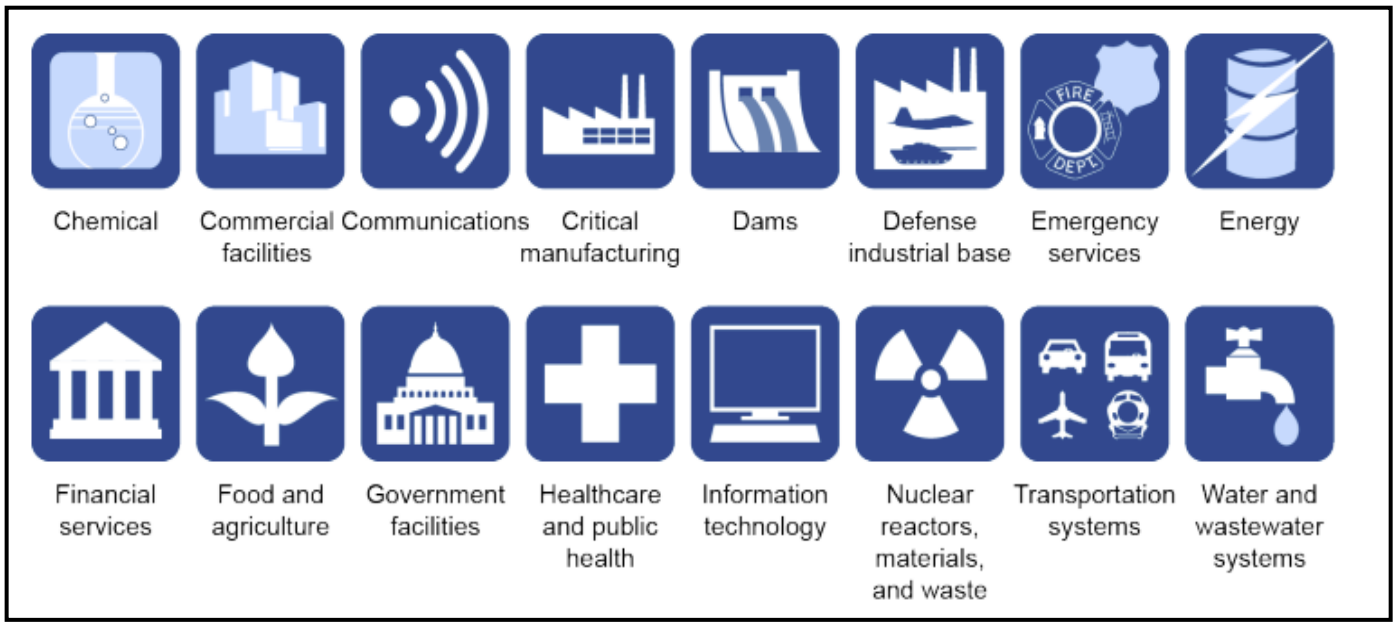
- ☐ Stock Price Reduction
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss, Devaluation Of Trade Names, Loss As A Leader In The Marketplace
- ☐ Compliance Fines, Data Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees / Lawsuits
- ☐ Increased Distrust / Erosion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



TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

- ☐ U.S. Government, State / City Governments
- ☐ Department of War, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports / Aviation (Pilots, Flight Attendants, Etc.)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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



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

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

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

What Do Employees' Do With The Money They Steal From Their Employers?
They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2026 REPORT ON FRAUD

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

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

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

Association of Certified Fraud Examiners 2026 Occupational Fraud Report Overview

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

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

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

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

Types Of Organizations Impacted By Fraud

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

Fraud At Federal / State Levels

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

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

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

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

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

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

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

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

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

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

Hotline Reporting / Fraud Awareness Training

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

Internal Control Weaknesses That Contribute To Fraud

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

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

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

Perpetrators Position

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

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

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

Perpetrators Tenure With Employer

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

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

Schemes Based On Perpetrators Department

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

Perpetrators Position Based Gender

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

Perpetrators Age

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

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

Perpetrators Education Level

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

Collusion By Multiple Perpetrators

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

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

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

Perpetrators Employment History / Criminal Background

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

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

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

Internal Actions Taken Against Perpetrators

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

Internal Punishment By Perpetrators Position

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

Litigation Against Perpetrators

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

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

Criminal Referrals Against Perpetrators

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

Reasons For Not Referring Fraud Case To Law Enforcement

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

Recovering Fraud Losses

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

Organization That Received Fines Because Of Employee Fraud

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

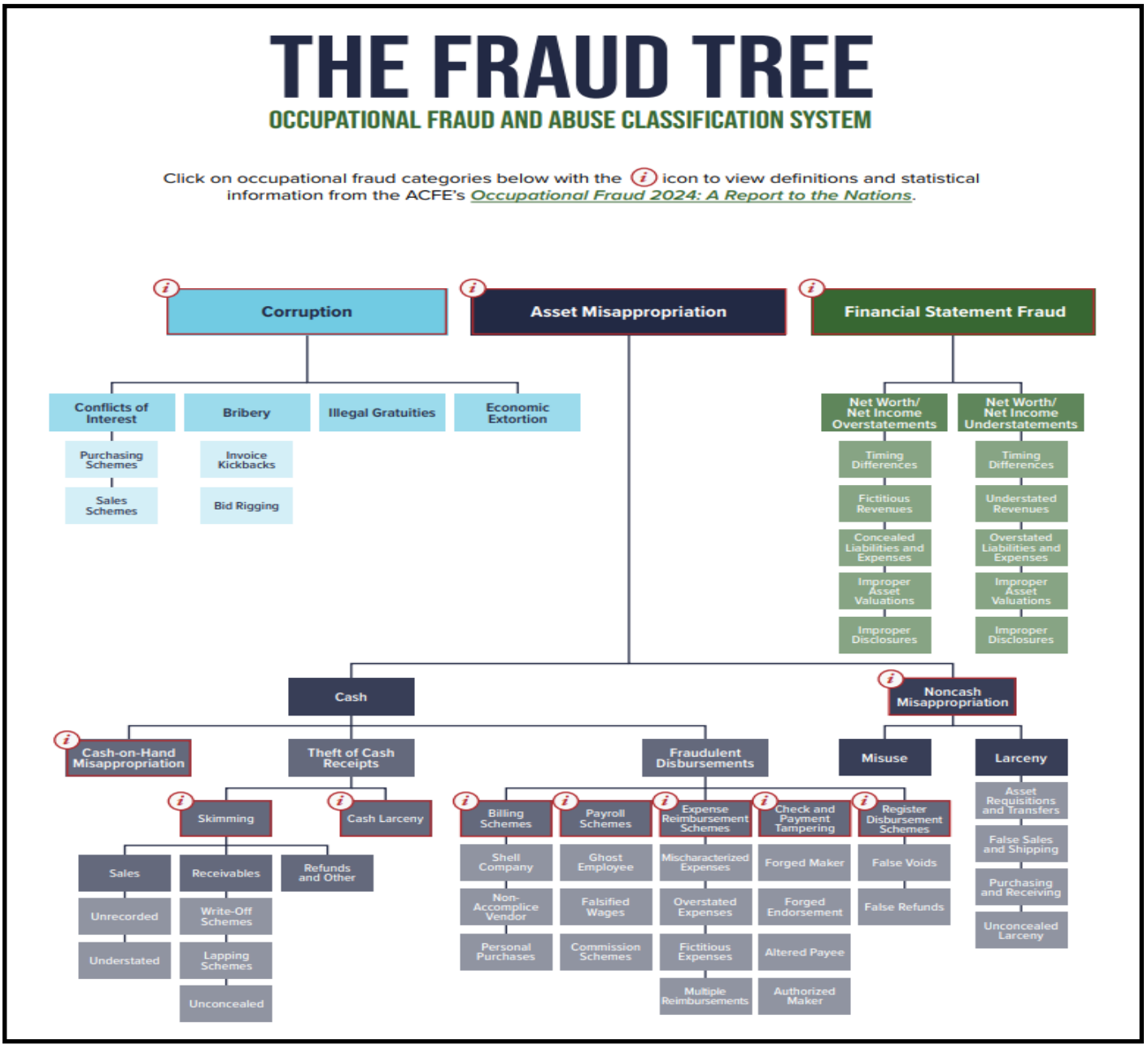
Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators



SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

TD Bank Pleads Guilty To Money Laundering Conspiracy / Employees Accepted $57,000+ In Bribes / FINED $1.8 BILLION - October 10, 2024

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB. Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TRADE SECRET THEFT / DATA BREACHES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy. Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees. Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis.

From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union.

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

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

Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business (2021)

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA.

From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

Controller Of Oil & Gas Company Sentenced To Prison For Role in $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers. Lyons initiated the fraud shortly after he became CEO in 1999.

In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

EMPLOYEE EXTORTION

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

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

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

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

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

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts.

Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)
Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data.

The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

Fired IT System Administrator Sabotages Railway Network - February 14, 2018
Christopher Grupe was suspended for 12 days back in December 2015 for insubordination while working for the Canadian Pacific Railway (CPR). When he returned the CPR had already decided they no longer wanted to work with Grupe and fired him. Grupe argued and got them to agree to let him resign. Little did CPR know, Grupe had no intention of going quietly.

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

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

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

IT Systems Administrator Sentenced To Prison For Hacking Computer Systems Of His Former Employer - Causing Company To Go Out Of Business (2010)
Dariusz Prugar worked as a IT Systems Administrator for an Internet Service Provider (Pa Online) until June 2010. But after a series of personal issues, he was let go.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

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

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

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired. On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

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

WORKPLACE VIOLENCE

Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024

Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours. Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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



NITSIG INSIDER THREAT SPECIALIZED REPORTS

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

INSIDER THREAT INCIDENTS E-MAGAZINE
2014 To Present / Updated Daily
The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**7,500+ Incidents**).

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X
Updated Daily
https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



NITSIG Overview

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

The NITSIG has been successful in bringing together a diverse group security professionals and individuals managing and supporting Insider Risk Management (IRM) Programs from the: U.S. Government Agencies, Department Of War, Intelligence Community Agencies, Critical Infrastructure Providers, Law Enforcement, Universities and Private Sector Businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM.

This has enabled the NITSIG membership to be much more effective in protecting their organizations assets against the severe impacts that can be caused by **Just 1 Employee**, **Multiple Employees In Collusion** or **Employees In Collusion With External Co-Conspirator(s)**. Many members have even stated the NITSIG is like having a team of IRM experts consultants at their disposal **FREE OF CHARGE**.

NITSIG Membership

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

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

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

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. The meetings are held at various locations throughout the U.S. See this link for some of the great speakers we have had at our meetings.

NITSIG Insider Threat Symposium & Expo (ITS&E)

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

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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a LinkedIn Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with **950+** members enables the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group.

NITSIG Advisory Board

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

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

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



INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

Since 2009, the Insider Threat Defense Group (ITDG) has provided **740+** organizations and **1100+** students with the core skills / advanced knowledge, resources and technical solutions for developing, managing, evaluating and optimizing their organizations Insider Risk Management (IRM) Programs (IRMP's).

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

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

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

IRMP TRAINING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

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

CONSULTING SERVICES OFFERED

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

BACKGROUND ON ITDG EXPERTISE IN THE FIELD OF INSIDER RISK MANAGEMENT

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

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

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

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

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

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

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

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

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

CLIENT SATISFACTION / COMPANY RECOGNITION

The comprehensive nature of our IRMP Framework and 15+ years of IRMP expertise, is what separates us from other providers of IRMP training and consulting services. ITDG training courses have been taught to over **1100+** individuals. Our students and clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM.

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

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

The ITDG Has Provided IRMP Training & Consulting Services To An Impressive List Of 740+ Clients:
White House, U.S. Capital Police, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. (Client Listing)

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

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

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
IRMP Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Threat Vulnerability Assessor & Mitigation Specialist
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG