

INSIDER THREAT INCIDENTS REPORT FOR

★ September 2026 ★

Fraud



Trade Secret Theft



Embezzlement



Classified Information Theft



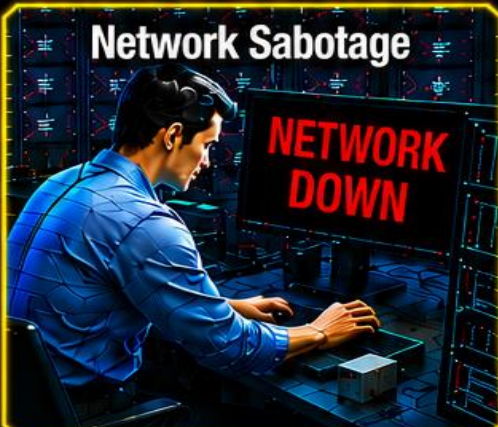
Bribery



Workplace Violence



Network Sabotage



Employee – Hacker Collusion



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

	<u>PAGE</u>
Insider Threat Incidents Report Overview	3
Insider Threat Incidents For September 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	40
Billion Dollar Impacts / Company Goes Out Of Business	
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 SEPTEMBER 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

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

[Insider Risks: A Diagnostic Tool To Detect & Preempt Non-Violent / Violent Insiders During Pre-Incident Phases - September 1, 2026](#)

U.S. GOVERNMENT

Former Homeland Security Employee Pleads Guilty To **\$250,000 Fraud Scheme By Holding 5 Different Jobs With Other U.S. Government Agencies - September 2, 2026**

Richeline Fung, 46, was a full-time DHS-CISA employee between September 2016 and October 2025. She lived in Maryland when she started working for DHS-CISA but moved to Florida.

Between January 2021 and August 2024, Fung served in multiple federal government contractor positions despite being a full-time U.S. government employee with DHS-CISA. She worked as a contractor for the Drug Enforcement Administration, Department of Energy, Department of Justice (DOJ), Federal Highway Administration (FHWA), U.S. Nuclear Regulatory Commission, and U.S. Department of Agriculture (USDA). She served in these positions as a direct employee or as an independent contractor / consultant through her business RAF Pro-Consulting, LLC, which she incorporated in Florida in 2020.

In connection with her employment, Fung submitted timesheets certifying the number of hours she worked each pay period. Fung routinely overstated those hours, even claiming to work more than 24 hours in a single day on multiple occasions.

For example, in February 2022, Fung was employed by DHS-CISA and three different federal contractors performing work for USDA, FHWA, and DOJ. For that month alone, Fung's combined hours totaled more than 24 hours in a single day on 15 occasions. Shockingly, she claimed to work 33 hours on February 7, 8, 9, and 10, and 32 hours on February 11.

Fung admitted that she concealed her employment with DHS-CISA and the federal contractors from each other. She also acknowledged that she was able to conceal her employment because she teleworked for all the positions during the relevant period. ([Source](#))

USDA Senior Director Sentenced To Prison For [Fraudulently Hiring Ghost Employee / Family Member & Paying Them \\$399,000+](#) - September 10, 2026

Kirk Perry, 62, is a former U.S. Department of Agriculture program director. He conspired to bill the federal government nearly \$400,000 for work that Jamarea Grant, 33 did not actually perform.

Grant's uncle is Perry. Perry used his position to secure employment for Grant as an Equal Opportunity Assistant. They billed the Office of the Assistant Secretary for Civil Rights and Grant received about \$399,319 from the government for work that was not performed.

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

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

Grant was ordered to pay restitution of \$399,319. ([Source](#))

Small Business Administration Employee Sentenced To Prison For [Taking Bribes In \\$3.5 Million COVID Fraud Scheme](#) - September 3, 2026

Attallah Williams, a former U.S. Small Business Administration (SBA) and Internal Revenue Service employee, has been sentenced to federal prison for taking bribes to submit and approve more than \$3.5 million in fraudulent pandemic relief payments. Williams orchestrated a three-year scheme to fraudulently obtain funds from four separate emergency pandemic relief programs:

First, Williams submitted fraudulent applications to the SBA to obtain Economic Injury Disaster Loans (EIDL) in the names of businesses that were not operational.

Second, Williams submitted a fraudulent application for a Paycheck Protection Program loan, guaranteed by the SBA, for a business that was not operational.

Third, Williams obtained a position as an SBA loan officer, enabling her to use her insider access to approve fraudulent applications to the EIDL Advance grant program. Williams advertised on Instagram to recruit accomplices who, under her guidance, submitted applications using the names of nonexistent or ineligible businesses. Williams then used her position to improperly approve those applications in exchange for a share of the proceeds. Williams also encouraged her conspirators to recruit additional participants, promising them referral fees for every person brought into the scheme.

Fourth, Williams left the SBA and obtained a position as an IRS tax examining technician. Williams again advertised on social media to recruit accomplices who, under her instructions and with her assistance, submitted fraudulent tax documents to the IRS to claim payments under the Employee Retention Tax Credit program, with Williams receiving a fee for each application.

In total, Williams submitted false claims for more than \$3.5 million of pandemic emergency assistance funds intended to help struggling businesses, resulting in \$3,272,000 being distributed before the scheme was disrupted. ([Source](#))

U.S. Postal Service Employee Sentenced To Prison For [Stealing Narcotic Prescriptions For U.S. Military Veterans](#) - September 21, 2026

Carrie Wallace, 48, used her position as a U.S. Postal Service employee to access and steal mail parcels containing prescription medication and vape products.

She intentionally targeted packages sent by the Department of Veterans Affairs to its patients because those packages generally contained narcotic medications. Wallace cut into the packages, opened the prescription narcotics medication bottles, stole the medication and replaced it with over-the-counter medication, retaped the packages and placed them back in the mail stream to be delivered to the intended recipients. Multiple veteran victims consumed the tampered medication, putting them at risk of injury for taking incorrectly dispensed drugs. Due to Wallace's medication theft and tampering, veteran victims experienced extreme pain, increased agitation, anger, and other mental health symptoms. ([Source](#))

U.S. Postal Service Employee [Given 3 Years Probation For Stealing \\$118,000+](#) - September 1, 2026

Between April 2025 and January 2026, while he was employed as the Postmaster of the Morrisville, New York, Post Office, Delos Thurston, 28, fraudulently issued 179 money orders for his own benefit without paying for them, and in so doing stole \$118,088.19 from the United States. Thurston was ordered to pay restitution to the U.S. Postal Service in the amount of \$118,088.19. ([Source](#))

U.S. Postal Service Employee Sentenced To Prison [For Attempted Destruction Of 498 Pieces of Mail Because She Did Not Wants To Deliver](#) - September 16, 2026

Stacy Braxton, 39, was a rural mail carrier for the Greenwood Post Office in Jackson County, Florida.

In February 2026, law enforcement recovered 498 pieces of mail from the defendant's mail route that were discarded in a burn barrel in Marianna, Florida. The defendant admitted to investigators that she attempted to discard and burn the mail from her route rather than delivering the mail to the designated recipients. ([Source](#))

U.S. Postal Employee Pleads Guilty To [Stealing Gift Cards From Mail](#) - September 16, 2026

Napeaches Blair, 43, has been a United States Postal Service employee for approximately eight years. An investigation revealed that the defendant had stolen numerous gift cards from outgoing mail in her capacity as a Postal employee.

In December 2025, the Blair intercepted two envelopes containing gift cards while at work. Blair removed the gift cards from the outgoing mail and then proceeded to use them at a store in Tallahassee and at a gas station in Quincy, Florida. Later, in July 2026, law enforcement observed Blair opening a letter, put \$1,000 in her pocket, and placed the empty envelope in an outgoing mail tub. Blair was placed under arrest, and law enforcement found the stolen \$1,000 in the Blair's pocket. Following the Blair's arrest, law enforcement conducted a search of her vehicle. Numerous gift cards were recovered. According to court records, law enforcement successfully identified several victims who had sent the gift cards before their mail was intercepted by Blair. Blair was also captured on security footage at various locations using the stolen gift cards while still dressed in her Postal employee uniform. ([Source](#))

U.S. Postal Service Employee [Charged With Dumping 30,000 Pieces Of Mail](#) - September 8, 2026

Armond Paige, 54, was indicted on one count of delay or destruction of mail by a postal employee.

Paige dumped mail in vacant, weedy lots rather than delivering it. From roughly 2024 to April 29, 2026, Paige discarded at least 30,000 pieces of mail in various vacant lots, the indictment says. At the time, Paige was working out of the Maryville Gardens Post Office on Meramec Street in south St. Louis. ([Source](#))

U.S. Mail Carrier [Charged For Failing To Deliver 8,500 Pieces OF Mail](#) - September 14, 2026

Ronald Juckno, 53, is former mail carrier for the U.S. Postal Service (USPS). He was arrested and charged with keeping and failing to deliver the mail.

Between August and September 2024, Juckno was found in possession of more than 8,500 pieces of mail that he had held onto and failed to deliver to his customers. The mail included sensitive items such as California EDD correspondence, financial records, insurance records, medical correspondence, tax records, and utility bills. He was placed on leave and then resigned his position as a mail carrier shortly after this discovery. ([Source](#))

U.S. Postal Service Employee Charged For [Disposing 300 Mail-In Ballots In Utah](#) - September 22, 2026

Damon Seei, 34, was charged as a former postman with the U.S. Postal Service with unlawful secretion, destruction, and delay of mail after he allegedly unlawfully threw away mail that he was entrusted to deliver, including approximately 300 mail-in ballots to registered voters in Utah. ([Source](#))

2 U.S. Postal Service Employees Charged With [Stealing 200+ Gift Cards Out Of The Mail](#) - September 25, 2026

Pian Wong-Tam is a former United States Postal Service (USPS) Mail Processing Clerk. William Wong is a former USPS Mail Clerk

Both engaged in a scheme and conspiracy in which Wong-Tam removed mail entrusted to her by USPS, stole gift cards and other items out of that mail. Wong-Tam shared the gift cards she stole with Wong and, together, they used those gift cards at a variety of businesses in multiple states for their own personal benefit. All told, Wong-Tam and Wong's scheme resulted in the theft of no less than 200 gift cards, ranging in value from \$25 to \$500 each. ([Source](#))

U.S. Postal Service Employee Pleads Guilty To [Stealing 141 Gift Cards](#) - September 24, 2026

David Boutte, 60, is an employee of the Blue Valley Post Office in Overland Park in Kansas.

In January 2026, the U.S. Postal Service - Office of Inspector General (USPS-OIG) received a tip from a witness who saw Boutte dispose of brightly colored envelopes which appeared to be for greeting cards into the trash bin outside his home. The witness looked in Boutte's trash and found four postmarked letters that were opened and not addressed to Boutte's home.

Twice in February 2026, USPS-OIG and the Olathe Police Department collected trash from the curb outside Boutte's home. Both times law enforcement found multiple opened, stamped letters not addressed to the residence.

In March, as officers executed search warrants at Boutte's home and at the post office, they found among his belongings \$1,624 in cash, 141 gift cards, letters addressed to other people, and approximately 1,700 stamps on rolls and sheets. They also found a USPS arrow key (a master key mail carriers use to open outdoor collection boxes, cluster box units, apartment mailbox panels) and a USPS facility key. ([Source](#))

Veterans Affairs Field Examiner Charged With Fraud For Obtaining \$101,000+ For COVID 19 PPP Loans - September 25, 2026

Between July 4, 2020, and October 13, 2021, Randy Bond, 52, carried out a scheme to defraud the federal government by submitting fraudulent Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) applications. In these submissions, Bond falsely claimed to own a car wash and automotive repair business generating substantial revenue, as well as a pet care business with significant monthly payroll expenses.

Bond allegedly applied for two EIDLs and two PPP loans, ultimately receiving approximately \$101,333. He is accused of using the funds for personal expenses, including purchases at Best Buy and Total Wine.

During the period of the fraud, Bond was employed full-time by the U.S. Department of Veterans Affairs as a field examiner, working with veterans who required fiduciary support. His responsibilities included meeting with veterans and their fiduciaries to ensure veterans were receiving proper care and reviewing accounting documentation when necessary. ([Source](#))

General Services Administration Contracting Officer Sentenced To Prison For Accepting \$50,000 In Bribes From Construction Companies - September 22, 2025

Between 2018 and 2021, Lennie Miller, 61, and Christopher Brackins, 53, knowingly and willfully conspired together for Miller to exercise his authority over the GSA contracting process. Through the scheme, Miller directed GSA federal project work to company A in exchange for cash and other things of value.

Miller effectively paired company A with prime contractors company B and company C to work on GSA federal projects. He solicited and accepted things of value, in return, from Brackins, including cash, checks, payments for repairs to his vehicle, and payments for repairs at a residence owned by Miller's relative.

Brackins provided Miller with approximately \$50,000 worth of money and other things of value. Bribery payments included, in late 2018, Brackins paying a fraudulently inflated bonus to one of his employees. Brackins then directed the employee to pay Miller \$8,000 in cash from the fraudulently inflated bonus check. Similarly, in early 2021, Brackins paid Miller \$25,000, at Miller's direction, using an intermediary who accepted the payments through the intermediary's air-conditioning repair business. ([Source](#))

U.S Department Of Agriculture Special Agent Charged With Fraudulently Obtaining \$51,000+ Of Disability Payments - September 29, 2026

Michelle Bouziden, 44, was an Assistant Special Agent in Charge for the U.S. Department of Agriculture Office of the Inspector General (USDA-OIG)

Bouziden suffered a concussion on the job in March 2026, but then beginning around May 14, 2026, she falsely reported that ongoing symptoms left her totally disabled and unable to work.

In filings with the Department of Labor (DOL) Office of Workers' Compensation Program, Bouziden sought disability pay claiming she was completely unable to engage in "arduous physical activity" and cognitive reasoning," and could not perform any required work tasks such as: sitting, walking, standing, twisting, bending, squatting, kneeling, climbing, and operating a motor vehicle. Bouziden received disability payments as she simultaneously traveled internationally and actively pursued a high-endurance, athletic lifestyle. Bouziden submitted documents to the DOL indicating she was totally disabled and too symptomatic to return to work on the same day she flew to Italy to hike the Dolomites. Bouziden allegedly remained in Italy for two weeks, hiking over 50 miles and documenting her experience on social media. Prior to leaving, Bouziden allegedly canceled a DOL appointment for a mandatory, independent second opinion medical evaluation claiming it conflicted with a "wellness retreat." The indictment alleges Bouziden received \$51,571.73 in disability compensation. ([Source](#))

U.S. Nuclear Regulatory Commission Employee Sentenced To Prison For \$20,000+ Time & Attendance Fraud Scheme - September 28, 2026

Evester Edd, 64, worked daily from his duty station at PC headquarters in Washington, D.C., or an alternate site, as the agency also allowed teleworking.

Beginning in September 2024, and continuing through November 2024, Edd falsely recorded work hours that he did not work in PC's time-and-attendance system. During this time frame, Edd submitted his time and attendance sheet electronically from his alternative telework duty station. The false entries resulted in PC paying Edd for hours he did not work.

After NRC OIG's Cyber Crimes Unit investigators analyzed Edd's NRC-issued laptop for the specified timeframe, they found that on nearly a daily basis, Edd signed on from his residence to work for the NRC during his PC work hours. Additionally, on nine of the days that he worked as a contractor, Edd, remotely signed into the NRC network but did work for the NRC while sitting in his workspace at PC headquarters during the PC workday.

Investigators also determined that Edd sent numerous government documents from the agencies' accounts to his personal AOL email account. Many documents were related to employment actions and included personally identifiable information (PII), along with other confidential details. ([Source](#))

DEPARTMENT OF WAR / INTELLIGENCE COMMUNITY

U.S. Army Soldier Pleads Guilty To Gathering & Transmitting National Defense Information To China With Help Of Other Soldiers - September 16, 2026

Between November 2021 and March 2025, within the District of Oregon and elsewhere, Ruoyu Duan, 41, conspired with others to surreptitiously gather sensitive military information related to the United States Army's operational capabilities, including computer equipment, training materials, intelligence reports, and technical manuals. Duan paid his co-conspirators, active-duty U.S. Army soldiers, and others, to gather information and equipment. Specifically, they obtained information related to U.S. military weapon systems, such as U.S. Army combat vehicles, including the Bradley, Stryker, and HIMARS platforms, and transferred that information to people in China.

Duan served as an U.S. Army soldier from 2013 – 2017 and was trained in the handling of sensitive and classified military information. ([Source](#))

U.S. Navy Sailors Plead Guilty To Selling Fentanyl-Laden Pills To Servicemembers On USS Abraham Lincoln Who Died - September 14, 2027

Former sailors Bailey Szramowski and Johnnese Poomaihealani pleaded guilty in federal court to selling counterfeit oxycodone pills containing fentanyl to active-duty U.S. Navy servicemembers stationed in San Diego, including during deployments.

Szramowski provided an active-duty U.S. Navy servicemember assigned to the USS Abraham Lincoln with 10 purported oxycodone pills in December 2022. The victim, identified in court records by his initials, A.N., overdosed and died of acute fentanyl intoxication in January 2023.

Despite knowing of A.N.'s death, Szramowski sold three more purported oxycodone pills to another sailor, identified as C.L., just 10 days later. After that sailor was taken to the hospital for a suspected overdose from which he recovered, Szramowski and Poomaihealani called C.L. and instructed C.L. to tell law enforcement he received the pills from A.N. and not Szramowski. ([Source](#))

Naval Information Warfare Center Employee Sentenced To Prison For [Accepting \\$209,000+ In Bribes For Contracts](#) - September 9, 2026

James Soriano, a former public official at the Naval Information Warfare Center in San Diego, was sentenced in federal court to 72 months in prison for accepting hundreds of thousands of dollars in bribes.

Soriano admitted he accepted bribes from defense contractors in the form of lavish meals, employment opportunities for family members and friends, and tickets to premier sporting events. In exchange, he used his position to help the contractors secure and maintain hundreds of millions of dollars in government contracts.

U.S. District Judge Todd W. Robinson ordered Soriano to forfeit \$209,527.51 and pay \$18,722.40 in restitution to the Internal Revenue Service.

According to Soriano's plea agreement, the defense contractors – acting through their presidents, officers, and employees – gave various things of value to Soriano, including dinners at Ruth's Chris, Island Prime, and Fogo de Chão; tickets to the 2018 MLB All-Star Game, 2018 World Series, and 2019 Superbowl; and jobs for Soriano's family and friends, including Soriano's wife and Soriano's family friend, Liberty Gutierrez, who gave Soriano \$2,000 a month in cash from her salary at one of the companies working under a defense contract.

In return, Soriano took official action to aid his benefactors, such as allowing defense contractors to draft government documents in competitive and non-competitive procurements, submitting those documents as part of the procurement process, and advocating for their selection as defense contractors. Soriano also willfully failed to disclose the cash payments he received from Gutierrez on his federal tax returns.

From approximately March 2016 through at least October 2019, Soriano and a coworker, Dawnell Parker, received bribes from Philip Flores, the president and CEO of Intellipeak Solutions, Inc., a defense contractor headquartered in Fredericksburg, Virginia.

Soriano also admitted that from approximately May 2015 through at least October 2019, he separately received bribes from another defense contractor, with offices in San Diego and Stafford, Virginia, who gave him things of value, such as expensive dinners, a job for his wife, and rounds of golf at a private country club.

From approximately June 2014 through at least October 2019, Soriano received bribes from Russell Thurston, the Vice President of Cambridge International Systems, Inc., a defense contractor headquartered in Arlington, Virginia. In return for these bribes, Soriano used various methods to steer contracts to these defense contractors and kept his contracting activities hidden from the Naval Information Warfare Center. ([Source](#))

Department Of War Contractor Pleads Guilty To [Embezzling \\$107,000+ Of Travel Reimbursement Funds](#) - September 16, 2026

Kevin Mickie, 47, was employed by a government contracting firm that provided technical support services to the Department of War, which uses the Defense Travel System (DTS) to manage, approve, and reimburse official government travel for authorized employees and personnel. From November 2019 through February 2023, Mickie managed DTS profiles with authority to view user accounts, reset credentials, and modify profile details, including changing bank account and disbursement information.

Mickie used his access to the DTS accounts to steal and divert \$107,316.82 in Department of War travel funds by replacing account holders' bank and routing numbers with his own, causing reimbursement payments to be disbursed via electronic funds transfers directly into Mickie's personal bank accounts. After modifying the traveler's DTS profile, Mickie completed the diversion by either modifying authorized travel vouchers to redirect a portion of legitimate travel reimbursement to himself or by creating fictitious travel authorizations and vouchers for travel that never occurred. Mickie also changed the primary e-mail address associated with the DTS accounts to his own e-mail address.

Although Mickie left his position with the contracting firm in February 2023, his scheme continued through January 2024 because several of the compromised DTS account holders were unaware portions of their travel were being diverted to Mickie's bank account. ([Source](#))

U.S. Army Pay Technician Sentenced To Prison For Fraudulently Claiming \$98,000+ For Military Funeral Honors Ceremonies That Never Occurred - September 8, 2026

A former Army pay technician (Christopher O'Connor), was sentenced to five years' probation, 100 hours of community service, and payment of \$98,691 in restitution.

O'Connor previously pleaded guilty to conspiracy, for submitting fraudulent reimbursement requests for military funeral honors that he and six other Army reservists allegedly performed, but had not. ([Source](#))

SECURITY CLEARANCE RELATED / WHISTLEBLOWERS

No Incidents To Report

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S. Customs Border Protection IT Supervisor Charged With Stealing Hardware From 46 Computers And Trading In To On-Line Retailer For Credit - September 12, 2026

The FBI has arrested and charged Terry "Jiajia" Liu, a Customs and Border Protection supervisor based in Calais, Maine, for theft and damage to government property.

Liu allegedly stole computer hardware, including Intel 14th Generation Raptor Lake Refresh processors, memory modules, and hard drives, from at least 46 Department of Homeland Security computers across three Maine border facilities. He replaced the stolen parts with inferior hardware and exchanged the stolen equipment through Newegg's trade-in program for store credit.

Liu's official responsibilities were limited to information-technology support, so they did not have access to modify any government computer.

Hidden surveillance cameras captured Liu opening government computers and swapping hardware during the midnight shift. Liu would take the systems to a training room to commit the crime.

One camera recording showed Liu using a screwdriver to scrape thermal paste off a processor and installing a replacement chip in one system. Meanwhile, another recording caught Liu removing a memory module from a system and storing it in their desk drawer.

Instead of trying to sell the stolen hardware on the open second-hand market, Liu used a less conspicuous approach: Newegg's Trade-In program. According to investigators, Liu sent 13 emails between a personal account and an official CBP email address containing shipping labels and trade-in receipts for processor models matching the missing components from the government computers.

Restoring the stolen hardware could cost about \$20,460, while fully replacing all 46 compromised computers with equivalent hardware would cost an estimated \$105,800. However, additional labor to configure each system for government use will drive the bill even higher. ([Source](#))

U.S. Citizenship & Immigration Services Contractor Employee Charged With Stealing Computer Hardware - September 17, 2026

Beginning in December 2025, the U.S. Citizenship and Immigration Services headquarters employed Bankole Akinfe, 49, as a contractor in its Information Technology Customer Support Center.

On August 27, 2026, Akinfe was observed removing at least 10 Random-Access Memory (RAM) modules from USCIS laptops without authorization. Akinfe was further observed putting the RAM modules in his pocket and taking them off the premises. ([Source](#))

U.S. Citizenship & Immigration Services Employee Charged For Accepting Hundreds Of Thousands Of Dollars In Payments In Exchange For Manipulating Immigration Applications - September 4, 2026

Lukman Ganiyu, a former Senior Immigration Services Officer with U.S. Citizenship and Immigration Services, and Adeniyi Somoye were arrested on federal charges for their roles in an alleged multi-year scheme to receive illegal gratuities in exchange for manipulating and expediting immigration applications.

The complaint alleges that Ganiyu and Somoye together collected hundreds of thousands of dollars in payments from applicants, several of which correspond directly with immigration approvals issued by Ganiyu.

Investigators also identified extensive WhatsApp communications between Ganiyu, Somoye and numerous applicants whose immigration cases they handled, including thousands of messages and hundreds of calls during the charged period. ([Source](#))

LAW FIRMS

No Incidents To Report

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

City Of Beverly Hills Employee Charged With The Misappropriation Of \$300,000+ - September 4, 2026

A former employee of the City of Beverly Hills has been indicted on multiple felony charges after an internal financial review exposed the alleged misappropriation of more than \$300,000 in municipal funds, Beverly Hills Police Chief Kory Martin announced Friday.

Shere Lomosad faces four felony charges following a months-long investigation, including two first-degree felonies: misapplication of fiduciary property and theft. Lomosad has also been charged with two counts of credit card abuse.

The investigation began in December 2025 when a city employee noticed irregularities in the city's financial records. Investigators believe the alleged financial activity began in 2024 and continued undetected until the discrepancy was raised late last year. The misuse involved "various methods," with a significant portion involving cash and other segments tied directly to the city's budget.

Following the initial discovery in December, Lomosad was placed on administrative leave and subsequently resigned from her position with the city. The City of Beverly Hills, which is entirely surrounded by Waco in McLennan County, has reportedly implemented operational changes to prevent a single individual from maintaining concentrated financial control in the future. ([Source](#))

Missouri Department Of Transportation Supervisor Charged For Using State Credit Cards To Make \$50,000+ In Personal Purchases - September 16, 2026

Artemus Jackson, 37, a former Missouri Department of Transportation (MODOT) supervisor at the Normandy, Missouri maintenance facility, has been indicted and accused of misusing state-issued credit cards to make \$50,000 in personal purchases, including watches, clothing, cologne, shoes, and accessories for his personal vehicles. Jackson misused MODOT issued credit cards from December 2022 through July 2026.

Jackson is also accused of stealing two newly purchased mowers and a newly purchased trailer from the MODOT maintenance facility, valued at nearly \$30,000.

Jackson made about 248 personal purchases using the cards, including electronic equipment, cologne, watches, clothing, shoes and equipment and accessories for his personal Yamaha Raptor ATV, Suzuki motorcycle and GMC Sierra 1500 truck, the indictment says. ([Source](#))

City Director Charged For Accepting \$20,000+ In Bribes Related To A Cannabis Business - September 24, 2026

kashawn McKinley, 42, is the Director of Constituent Services in Atlantic City and a member of the Atlantic City School Board,.

McKinley solicited more than \$20,000 in cash and marijuana in exchange for his official assistance to a cannabis business owner in connection with the opening of the business and resolving certain fees owed by the business owner to the City of Atlantic City. In one instance, McKinley received a bribe payment for his assistance in getting the cannabis business classified as a “micro” cannabis business instead of a standard cannabis business, which resulted in the business paying a \$2,500 annual fee to renew its mercantile license instead of the \$25,000 annual fee required for standard cannabis businesses.

In addition to receiving cash and cannabis, McKinley in one instance expected payment in the form of services. Specifically, in October 2025, McKinley directed the business owner to assault another person in exchange for McKinley’s official assistance in resolving the fee disputes between the business owner and Atlantic City. When McKinley was later shown what appeared to be a photograph of the injured victim, McKinley expressed pleasure and assured the cannabis business owner that when it came to the fee disputes with Atlantic City: “you don’t have to worry about nothing.” ([Source](#))

SCHOOL SYSTEMS / UNIVERSITIES

Ohio State University Agrees To \$2.1 Million Settlement To Resolve Allegations That It Failed To Disclose Employees’ Ties To People’s Republic Of China - August 31, 2026

Ohio State University (OSU), a public university in Columbus, Ohio, has agreed to pay a total of \$2,100,000 to resolve civil allegations that it failed to disclose OSU employees’ affiliations with and support from the People’s Republic of China (PRC) in connection with federal research funding.

This settlement relates to National Aeronautics and Space Administration (NASA) and National Science Foundation (NSF) grants that provided funding to OSU from November 2012 to August 2023.

In the funding application process, NASA and NSF required OSU to disclose, among other things, foreign government support received by any principal investigator (PI) or co-PI on the grant application. Further, since 2011, federal law prohibits the use of grant funds for collaborations with the PRC, PRC Universities, or any PRC-owned companies. The settlement resolves allegations that OSU failed to disclose the collaboration and affiliation with, or funding received from, the PRC by certain OSU employees working on NASA and NSF grants.

Specifically, the settlement resolves allegations that since 2014, annual Faculty Activity Reports submitted to OSU identified affiliations with PRC universities and state-run research organizations, but OSU did not disclose this information to NASA or NSF.

In addition, OSU learned in 2019 that a PI on NASA grants was a participant in a Thousand Talents Program, a program established by the PRC to recruit individuals with knowledge or access to foreign technology intellectual property, but OSU did not notify NASA or NSF until four years later in 2023. The United States identified additional OSU employees who worked on those grants and were affiliated with, or collaborated with, or received funding from, the PRC. ([Source](#))

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank CEO Sentenced To Prison For Role In \$24 Million+ Wire Fraud Conspiracy That Caused Bank To Collapse - September 21, 2026

Tomás Concha, 64, a Spanish and Venezuelan national, is the former chief executive officer of Nodus International Bank (Nodus Bank), a Puerto Rican international bank.

Concha led a scheme to fraudulently obtain at least \$24.9 million from Nodus Bank and conspired to evade U.S. sanctions against Venezuela. Niembro was ordered to forfeit over \$16.9 million, which represents the value of the proceeds he derived from the wire fraud conspiracy.

Concha conspired with others to siphon money from Nodus Bank, ultimately leading to the bank's failure in 2023. Concha and his co-conspirators concealed from other Nodus Bank board members, executives and the bank's regulator, OCIF, that certain investments and loans were for the benefit of Concha and Board Chairman Juan Ramirez, in violation of Puerto Rican law.

From 2017 to 2023, Concha, Ramirez and others caused Nodus Bank to invest \$11 million in a Miami-based lender so those funds could be loaned to Concha and Ramirez for their own benefit. Conch and his co-conspirators knew that these transactions were illegal and concealed their conduct through the sham investments.

Between January 2018 and September 2021, Niembro and Ramirez also fraudulently induced Nodus Bank's board and comptroller to agree to buy at least 47 promissory notes totaling approximately \$25.3 million from Nodus Finance, a Miami-based company that Niembro and Ramirez jointly owned, so they could use the proceeds of the transactions for themselves. ([Source](#))

Bank Vice President Pleads Guilty To \$4.4 Million+ Financial Fraud Scheme - September 9, 2026

Craig Johnson, 45, was hired at Community First Bank in 2022 as a Vice President and Loan Officer. While Johnson was employed with Community First Bank, Johnson was also a pastor with a church in El Dorado Springs, Mo. until he was removed in 2025.

Beginning in at least 2024, Johnson began to request "investments" from various individuals for the purpose of buying cattle which would be later sold for profit.

The deal varied from person to person but involved Johnson purchasing cattle and selling the cattle for a profit within a short time frame. Johnson told individuals he needed help investing and requested they pay him funds.

Johnson worked with some of the “investors” to take out a loan at Community First Bank through Johnson and give the proceeds to Johnson. Johnson did not tell anyone at Community First Bank that he was benefiting from the loan proceeds.

Johnson did not use the funds to purchase cattle but instead deposited the funds in an investment account where he repeatedly traded in small-capitalization and micro-cap securities ultimately losing all the funds. Johnson served as loan officer for approximately 29 loans and lines of credit at Community First Bank totaling approximately \$4,476,156.22.

After receiving the victims’ funds, Johnson did not use the funds for proposed cattle sales. Instead, he used the victims’ funds to invest in high-risk stocks via his personal investment account. To further and conceal his scheme, Johnson used some of the victim’s funds to pay earlier investors in the scheme. ([Source](#))

Banking Employee Sentenced To Prison For \$2.2 Million Fraudulent Covid Loans Scheme & For Receiving \$200,000+ In Bribes - September 18, 2026

A 38-year-old Houston man (Feliciano Pineda) has been ordered to federal prison for conspiring to defraud his former employer through fraudulent Paycheck Protection Program (PPP) loans.

Pineda worked at a Houston bank at the start of the COVID-19 pandemic. From April through August 2020, he used his position to process fraudulent PPP loans for businesses that did not qualify because they either did not exist or had falsely inflated their financial information.

Pineda admitted to creating a fake LLC and opening a business bank account to receive kickback checks from customers he helped obtain fraudulent loans. Pineda was also ordered to pay approximately \$2.2 million in total restitution to his victims. Pineda personally benefited from the scheme, receiving more than \$200,000 in loan proceeds from borrowers whose PPP loans he helped facilitate. ([Source](#))

Bank Teller Charged With Stealing \$931,000+ From Customer Accounts - September 28, 2026

In 2021, Ameris Bank employed Mercedes Henry as a universal banker at Ameris Bank at multiple locations in the Atlanta area.

On at least six occasions from September 2021 to November 2021, Henry allegedly used six Ameris customers’ bank account numbers and identifiers to link the customers’ Ameris accounts to accounts at Coinbase, a cryptocurrency exchange platform that allows account holders to buy different cryptocurrencies, such as Bitcoin. Through this scheme, Henry and her conspirators caused the fraudulent transfer of approximately \$931,500 from victims’ accounts at Ameris Bank to Coinbase accounts controlled by the conspirators. Henry received more than \$1,000 in exchange for her participation in the scheme. ([Source](#))

Bank Employee Sentenced To Prison For Targeting 100+ Elderly Victims & Stealing \$2 Million In Identity Theft & Fraud Scheme - September 17, 2026

Yue Cao was Chinese national working for an Ohio bank.

Cao was a quant analytics manager at the based bank who was hired to help protect customers from fraud. He instead used his access to steal the identities and money of elderly customers who had not enrolled in the bank’s online services. He used an offshore service to create email addresses in the names of more than 100 victims.

Then, he used these emails to enroll the victims in online banking—all without their knowledge or authorization. Additionally, Cao directed the victims' bank statements and other notifications to the email addresses he created.

Because he controlled their online banking, he transferred the victims' money directly to his personal bank and credit card accounts.

He also used the victims' identities to open bank accounts in their names without their knowledge and transferred their money into them. Some of these were brokerage accounts, where he then engaged in options trading using their money.

The victims targeted by Cao's scheme resided in the states of New York, Pennsylvania, Connecticut, Washington, and Ohio (Canton in Stark County) and ranged in age from 90-103 years old at the time that Cao secretly enrolled them in online banking. In total, he conducted approximately \$2 million in unauthorized transfers using his control of the victims' accounts. ([Source](#))

Credit Union Loan Officer Sentenced To Prison [For Embezzling \\$171,000](#) - September 1, 2026

Ricky Naovoravong, 39, was a loan officer at a credit union in Garden City, Kansas.

In August 2024, a manager noticed a suspicious transfer from a member's savings account into Naovoravong's checking account. The manager noted that Naovoravong created documents for a \$5,000 loan in the victim's name then used the victim's account to make loan payments that would be deposited into his account.

A broader investigation ensued and determined Naovoravong had created other loans and transferred funds into his personal account. When confronted, Naovoravong admitted the loans were fictitious, and the victims knew nothing of them.

He said he would continue to create new fictitious loans to make payments on previous fictitious loans so that members wouldn't be notified of the loans. Naovoravong embezzled \$171,164 between November 2020 and August 2024. ([Source](#))

PHARMACEUTICAL COMPANIES / PHARMACIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES / MEDICARE FRAUD

Pharmacist For National Pharmacy Chain Pleads Guilty To [Drug Diversion For His Own Use](#) - September 18, 2026

A pharmacist Joshua Bradley, 30, pleaded guilty in federal court in Boston to diverting Adderall and Dextroamp-amphetamin (generic Adderall) from a national pharmacy chain.

While working as a licensed pharmacist Bradley diverted various quantities of Dextroamp-amphetamin for his own use on four occasions in August, September and November 2024. Additionally, on Nov. 10, 2024, Bradley also diverted Adderall. These controlled substances originally were intended for customers. ([Source](#))

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

[Weekly EchoMark Listing Of Employee Data Leaks](#)

Citizens Bank Is Suing A Rival Lender Alleging SoFi Bank Hired 30 Citizens Employees & Stole Trade Secrets - September 13, 2026

Nine members of Citizens' Connecticut mortgage operation resigned June 12 and joined SoFi, according to the federal lawsuit. The group included a manager and loan officers responsible for more than \$400 million in closed loans over the previous year.

Citizens alleges SoFi recruited 70% of its Connecticut mortgage producers, who had closed more than 80% of the bank's Connecticut mortgages during the year before their departures.

The lawsuit does not contend that hiring a competitor's employees is inherently unlawful. Rather, Citizens alleges SoFi encouraged former employees to breach contractual restrictions on soliciting co-workers and customers and to remove confidential information that could be used to compete for business.

The Rhode Island-based bank, a subsidiary of Citizens Financial Group Inc., alleges SoFi has hired more than 30 of its mortgage employees nationwide since August 2024. Citizens says the departures have "decimated" its Connecticut mortgage business and "essentially eliminated its market presence" in the state.

Citizens claims the departures were coordinated to cause maximum disruption to its Connecticut mortgage operation. It alleges SoFi knew that the former employees had agreements containing confidentiality provisions and restrictions on soliciting Citizens employees and customers. SoFi's recruitment extended beyond Connecticut, Citizens alleges, citing departures from its mortgage operations in Arizona, Florida, Minnesota, New York, Pennsylvania, Tennessee, Texas and Virginia.

Citizens traces the alleged campaign to August 2024, when its executive vice president and head of consumer lending left the bank for a similar position at SoFi, according to the complaint.

Citizens also alleges former employees removed confidential information around the time of their resignations and that SoFi encouraged, obtained and used the information to compete for customers.

A forensic review found client lists sent to personal email accounts, a spreadsheet containing customer contacts and real estate agent referrals, an attempted upload of client data to a personal iCloud account, and a loan pipeline report printed on the day of the Connecticut resignations, according to the complaint. The bank alleges the information included customer names, contact information, account numbers, loan amounts and rates, credit details, referral sources, pricing models and refinancing information.

Citizens says it sent cease-and-desist letters to the departing Connecticut employees but received no response from them or SoFi.

The 10-count lawsuit accuses SoFi of obtaining and using Citizens' trade secrets without authorization, interfering with the bank's employment contracts and customer relationships, and helping former employees violate duties they owed Citizens. Citizens also alleges SoFi conspired with the former employees to compete unfairly. The claims were brought under federal and state trade-secret laws, Connecticut's unfair trade practices law and the federal racketeering law known as RICO. ([Source](#))

2 Former Employees Of Elevance Health Being Sued For Soliciting Employees To Join Them At New Company And Steal Proprietary Information - September 4, 2026

Elevance Health brings this action to halt an unlawful scheme orchestrated by its competitor, Senderra, and several former Elevance Health employees (Derek Ormond, Eric Mitchell).

While still employed by Elevance Health and continuing after their departures, these employees conspired with Senderra to target Elevance Health's 340B specialty pharmacy business, BioPlus. Defendants raided BioPlus's workforce, diverted its customers, and misappropriated its confidential and proprietary information, all in flagrant violation of their contractual, fiduciary, and statutory duties, and well beyond the bounds of lawful competition. ([Source](#))

Lawsuit Filed Against Vice President Of Healthcare Networks At Elevance Health For Stealing Trade Secrets - September 9, 2026

The lawsuit seeks an injunction regarding the misappropriation of trade secrets by Jordan Vidor who worked for Elevance Health. Elevance Health submitted multiple exhibits alongside the complaint, including Vidor's employment, executive, and stock agreements. Elevance Health alleges that Vidor took confidential and trade secret information to join competitor Oscar Health. ([Source](#))

Chief Investment Officer For Financial Firm Resigns, Steals Trade Secrets & Begins Soliciting Clients From Previous Employer - September 24, 2026

Stephan A. Colglazier, former Chief Investment Officer of Sharp Financial, resigned on August 12, 2026, and immediately began soliciting Sharp Financial's clients for his new employer ASE, a competitor.

Prior to resignation, he emailed Sharp Financial documents to his personal email and surgically deleted emails from his Sharp Financial account. Sharp Financial alleges he misappropriated trade secrets including Model Strategies, Strategic Asset Management platform, and Tactical Asset Management platform, and used them to benefit ASE and Belpointe while harming Sharp Financial. ([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 Incidents 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>

Lyft Driver Terminated For Using Google Gemini AI To Produce Fraudulent Document - May 20, 2026

A Lyft driver in Boca Raton, Florida, allegedly submitted an AI-generated image showing spilled food and drink to support a \$75 damage fee against teenage passengers. The riders' family identified a Google Gemini logo in the image and disputed the claim. Lyft later acknowledged the image was AI-generated, reimbursed the charge, and removed the driver from the platform. ([Source](#))

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

No Incidents To Report

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 /

Energy Trader For Vitol Sentenced To Prison For \$500 Million International Bribery Scheme Involving 7 Co-Conspirators - September 18, 2026

Between 2015 and 2020, Javier Aguilar was a trader in the Houston office of Vitol, Inc. (Vitol), the U.S. affiliate of the Vitol group of companies, which together form one of the world's largest energy trading firms.

As part of the scheme, Aguilar and his co-conspirators agreed to bribe senior Ecuadorian officials to obtain a \$300 million contract to purchase fuel oil for Vitol. Aguilar and his co-conspirators used another Middle Eastern state-owned entity to circumvent Petroecuador's restrictions on contracts with private companies. In return for the promise and payments of bribes, the Ecuadorian officials then ensured that the Middle Eastern state-owned entity and Vitol were awarded the contract.

To conceal the scheme, Aguilar and his co-conspirators used a series of fake contracts, sham invoices, and shell entities incorporated in Curacao, Panama, and Cayman Islands.

Aguilar also used alias email accounts to communicate with his co-conspirators. The evidence at trial also demonstrated that Aguilar used the same system of shell entities and sham invoices to launder bribe payments to two officials at PPI. In total, Aguilar paid approximately \$600,000 in bribes to PPI officials to obtain contracts for Vitol to supply hundreds of millions of dollars of ethane gas to PEMEX.

Seven of Aguilar's co-conspirators, including three foreign government officials, have pleaded guilty for their roles in the schemes. These individuals have collectively agreed to forfeit more than \$63 million in proceeds from the schemes.

In December 2020, Vitol admitted to bribing officials in Ecuador, Mexico, and Brazil in violation of the anti-bribery provisions of the FCPA. Vitol entered into a deferred prosecution agreement with the U.S. Attorney's Office for the Eastern District of New York and the Criminal Division's White Collar and Corporate Enforcement Section. As a part of the resolution, Vitol agreed to pay a combined \$135 million in penalties as part of a coordinated resolution with the Justice Department, the Commodity Futures Trading Commission, and authorities in Brazil. ([Source](#))

Mexican National Working For U.S. Aerospace Manufacture Charged With Fraud, False Claims Of U.S. Citizenship & Identity Theft - September 18, 2026

A Mexican national (Alma Villafana, 54) who decades ago was ordered removed from the United States was arrested on an eight-count federal grand jury indictment charging her with securing her employment at a South Bay aerospace manufacturer and U.S. military contractor by lying on an employment authorization form that she was a U.S. citizen and by submitting someone else's legitimate certificate of naturalization number.

Villafana is charged with five counts of wire fraud, one count of use of a false and forged certificate of naturalization, one count of aggravated identity theft, and one count of false claim to United States citizenship.

In December 1996, Villafana secured employment at a Torrance-based business identified in court documents as Company-2, in part, by attesting on her Form I-9 that she was a U.S. citizen. In fact, Villafana is an illegal alien from Mexico who in 2003 was ordered by an immigration judge to be removed from the United States.

In January 2026, Villafana again knowingly submitted a Form I-9 falsely attesting under penalty of perjury that she was a U.S. citizen to maintain her employment at a business identified in court documents as Company-1.

As part of the Form I-9, she also knowingly provided a certificate of naturalization number that belonged to another person. From December 1996 to September 2026, Villafana obtained at least \$1,402,459 in payment for her employment at Company-2 and Company-1, included by direct deposit wired to her bank account. ([Source](#))

Company Employee For Scrap Metal Business Sentenced To Prison For [Stealing \\$481,000+](#) - September 24, 2026

Tanya Januszewski worked as a cashier for a local scrap metal business and used her position to defraud the company out of hundreds of thousands of dollars.

From October 2022 to June 2024, Januszewski created hundreds of false transaction records in the company's electronic sales records and stole cash from the company's cash drawer in amounts matching each false transaction. Over the course of her scheme, Januszewski defrauded the company out of \$481,197, and she was ordered to repay the company. ([Source](#))

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

Office Manager For Medical Practice Sentenced To Prison For [Embezzling \\$7.8 Million From 2 Practices / Used Funds To Pay Credit Card Debit, Upgrade Home, Etc.](#) - September 2, 2026

Adam Gentile, 40 was hired as an administrative assistant for a medical practice near Boston around 2014, Gentile He was promoted to the role of office manager shortly thereafter. In his capacity as office manager, Gentile processed payroll and oversaw other recordkeeping and administrative responsibilities for the practice.

Beginning in or around 2015 and continuing through November 2020, Gentile embezzled more than \$4.5 million from his employer by issuing himself extra paychecks, sometimes labeling the payments as "bonuses." Gentile also paid off personal credit cards with the practice's bank account.

In 2021, Gentile was hired as an officer manager for a second medical practice, for which he similarly had sole responsibility for processing payroll.

From in or around April 2021 through May 2024, Gentile executed a similar scheme in which he caused extra payroll payments to be issued to himself – sometimes recording these payments as "bonuses."

Gentile used the employer's bank account to pay off his personal credit cards; purchase and upgrade his home in Hudson; and put toward a side business he ran while employed by the medical practice. Gentile embezzled more than \$3.3 million from his second employer. Gentile was ordered to pay forfeiture in the amount of \$7.8 million. ([Source](#))

Business Bookkeeper Arrested For [Making \\$4 Million+ Of Unauthorized Purchases Using Employers Credit Card / Used Funds For Luxury Lifestyle, Motorcycle & Truck](#) - September 8, 2026

Between November 2020 and October 2024, Kelly Brown, 47, worked as a bookkeeper at a leading Fresno, California business specializing in custom countertops and commercial hardwood products. In her role, she had access to the personally identifiable information of employees, including the business's owner.

In January 2021, Brown recommended that the owner obtain an American Express credit card for business expenses.

The owner, however, was not interested in obtaining an American Express credit card for himself or for his business. Nevertheless, two weeks later Brown gave the owner two American Express credit cards, one under the owner's personal name and the other under the business name.

A few months later and unbeknownst to the owner, Brown obtained a credit card in her own name under the owner's American Express account without his authorization. Brown began using this credit card for unauthorized personal expenses, including luxury retail purchases, travel, health and beauty treatments, and a down payment on a 2022 Harley-Davidson motorcycle and a 2023 Chevrolet Silverado 2500.

In August 2022, Brown started an online apparel store, Western Edge Boutique. Around the same time, she made numerous clothing and apparel-related purchases on the unauthorized card.

Brown used the business's bank account to make payments to American Express from 2021 through 2024 to conceal and further her fraud scheme. In late 2024, the owner discovered the scheme and fired Brown. Brown spent more than \$4 million dollars on unauthorized purchases. ([Source](#))

Business Executive Manager Pleads Guilty To [Stealing \\$2.3 Million+ / Used Funds For Gambling - September 21, 2026](#)

Between February 2023 and July 2025, while working as an Executive Manager at a business in California, Christopher Abplanalp, 38, stole more than \$2.3 million, most of which he then spent gambling.

In executing the scheme, he diverted money from the business's account with an online payment processing system to his own personal account, or to various other friends or acquaintances. Abplanalp also repeatedly charged a client's credit card for items the client never ordered and for invoices that did not exist, then transferred those proceeds to himself. Additionally, he instructed clients to tender payments directly to him and told vendors to issue rebates and refunds to his personal account, rather than the business. To conceal his theft, Abplanalp altered, deleted, or made false entries to the business's accounting software. ([Source](#))

Health Care Products & Services Manager Sentenced To Prison For [Embezzling \\$1.6 Million+ Over 4 Years / Used Funds For Wedding, Vacations, Etc. - September 24, 2026](#)

Tony Ream was employed by a company headquartered in Melville, New York that is a distributor of health care products and services, and serves as the world's largest provider of health care solutions to office-based dental and medical practitioners worldwide. Ream was hired by the company in 2019 to work in its credit department and became a credit supervisor.

From approximately October 2020 through November 2024, Ream siphoned corporate funds from customer refund accounts, some of which were inactive, and diverted the funds to his own personal accounts, masking the fraud by recording each transaction as a refund that was issued to a customer. Ream also deceived his subordinates into unwittingly taking steps that facilitated his embezzlement scheme. In total, Ream embezzled approximately \$1.6 million from the company, which he spent on his wedding, luxury international vacations, and a failed restaurant venture in South Carolina. ([Source](#))

Human Resources Manager Sentenced To Prison For [Embezzling \\$1.2 Million+ From Employer / Used Funds For Gambling - September 22, 2026](#)

Beginning in 2017 and continuing through May 2025, Brigit Marshall, 49, embezzled over \$1.2 million from her employer, a company headquartered in Minnesota that sells new trucks, parts, and services. The defendant worked at the company beginning in 2017. Her job included overseeing human resources and doing the company's payroll. Marshall began creating excess garnishments within the payroll system and directed, via electronic bank transfer, these fabricated garnishments to herself or accounts she controlled.

To cover up her embezzlement scheme, Marshall created separate general ledgers, and the transfer of these embezzled funds were hidden or buried in legitimate payments in unrelated areas. The defendant used the fraudulently obtained funds for personal spending and to fund her gambling addiction. ([Source](#))

Bookkeeper Working For 3 Businesses Sentenced To Prison For [Stealing \\$595,000+ / Used Funds For Home Remodeling, Trips, Etc. - September 17, 2026](#)

During three separate periods between June 2021 and February 2025, Monica Padilla, 49, worked as a bookkeeper for multiple businesses. As bookkeeper, Padilla had access to bank and credit accounts.

At each of the three employers, Padilla used various methods to fraudulently steal funds from the accounts. With the stolen money, Padilla remodeled her home, purchased Disney merchandise, bought hundreds of DoorDash orders, and funded her daughter's cheerleading activities along with a more than \$5,700 trip to California.

Padilla was first charged in a 30-count indictment on Aug. 16, 2023, then in an 18-count superseding indictment on Feb. 19, 2025, both of which included more than a dozen wire fraud counts. While on pretrial release after the February 2025 superseding indictment, Padilla violated her bond conditions, lied to pretrial services, and obtained employment as a remote bookkeeper for an accounting firm, where she again defrauded her employer and her employer's clients. Throughout Padilla's multi-year criminal scheme, she defrauded three separate businesses for a total loss of at least \$595,585.41. ([Source](#))

Business Bookkeeper For 40+ Years Pleads Guilty To [Stealing \\$205,000+ / Used Funds For Credit Card Payments, Amazon Purchases, Etc. - September 14, 2026](#)

Angela Conley, 60, worked as the bookkeeper for a Virginia-based business for more than 40 years until she was terminated in February 2025. As the company's bookkeeper, Conley was responsible for the company's and had access to bank accounts and was issued a company credit card.

Beginning in January 2020 and continuing through February 2025, Conley devised a scheme to personally enrich herself through fraud by obtaining funds that belonged to the company. Conley sent wire transfers of funds from the company's bank account to Conley's personal Capital One credit card account, her personal checking account, and to make hundreds of purchases from Amazon. These 474 items included high heel shoes, pool covers, and earrings. All of the items were delivered via the U.S. Postal Service or commercial interstate carrier.

Conley sent 38 payments totaling \$139,246 from Company A's bank account to her personal credit card account without authorization.

In addition, Conley transferred funds from Company A's bank account to Verizon, BVU Authority, and the Virginia Department of Taxation as payment for Conley's personal bills. All these payments were made without authorization. In all, between January 2020 and February 2025, Conley caused \$205,889 in fraudulent transactions to be made. ([Source](#))

Chief Financial Officer For Organization That Received Federal Funds Pleads [Guilty To Stealing \\$162,000+ / Used Funds For Travel, Cosmetic Dermatologist, Etc. - September 4, 2026](#)

Rachel Crawford, 47, was the Chief Financial Officer of an organization that received federal funds.

Beginning on or about May 14, 2021, and continuing until or about May 8, 2025, Crawford withdrew approximately \$162,209.61 in cash from the organization's checking account for personal use. Crawford then altered bank statements to conceal her withdrawals. In addition, Crawford made \$9,254.81 of unauthorized purchases for personal items, including airplane tickets and a cosmetic dermatologist, using the organization's credit card. When interviewed by federal agents, Crawford admitted to the scheme. ([Source](#))

Employee Of Child Advocacy Nonprofit Pleads Guilty To Embezzling \$96,000+ / Used Funds For Personal Bills, Home Theater Equipment, Etc. - September 15, 2026

Jennifer O'Neal, a former program specialist for a nonprofit corporation serving abused and neglected children, pled guilty to stealing \$96,713 from CASA of Polk & Haralson in Georgia.

CASA of Polk & Haralson employed O'Neal as a program specialist in charge of processing payroll and expense reimbursements for staff and volunteers. From 2018 to 2022, O'Neal issued frequent fraudulent payments to herself and others from CASA's bank accounts that were not for legitimate CASA expenses.

Some of the improper payments were disguised as mileage payments for travel to court appearances or conferences, or expense reimbursements for restaurants, groceries, utilities, and clothes purportedly for volunteers, staff, and children.

However, the mileage charges were inflated or were based on travel that did not occur, and the restaurant, grocery, utilities, and clothes reimbursements were made for O'Neal's personal expenses. For example, O'Neal used CASA funds to pay for her own power, water/sewage, and cell phone bills. Some payments covered charges at a Six Flags amusement park, a Netflix subscription, and purchases of softball gear and lingerie. O'Neal also issued payments purportedly for office supplies but used to purchase home theater equipment that she installed at her residence. ([Source](#))

Director Of State Housing Authority Pleads Guilty To Stealing \$6,200+ To Remodel Home Master Bathroom - August 31, 2026

Michael Lara, 41, of Norwood, Mass., was charged with one count of wire fraud. Lara has agreed to plead guilty and entered into a Deferred Prosecution Agreement (DPA) with the U.S. Attorney's Office. Under the terms of the DPA, Lara has agreed to repay over \$6,200 stolen from the Watertown Housing Authority (WHA), and will resign from his current position as the Executive Director of the Newton Housing Authority.

Lara was the Executive Director of WHA and president of both the Watertown Housing Development Corporation (WHDC) and WHDC Holdings, LLC from July 2019 to January 2025. As the Executive Director, Lara had access to WHA's charge account with Home Depot as well as WHDC's credit cards.

Per WHA policy, WHA credit cards can only be used for the purchases of goods and services that are the official business of the WHA. Despite the policy, Lara made a series of personal purchases beginning in 2022 using WHA and WHDC funds. Specifically, in 2023, Lara began a master bathroom renovation and used WHA and WHDC funds to buy fixtures for his bathroom. ([Source](#))

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

IT Manager Sentenced To Prison For Embezzling Nearly \$1 Million from Employer Using Shell Company & Fraudulent Invoices - September 8, 2026

Charles A. Richardson, 45, was employed as an information technology professional with the Pittsburgh-based philanthropic foundation The Heinz Endowments.

Between 2016 and 2024, Richardson embezzled nearly \$1 million in funds from his employer through a shell corporation Richardson controlled by authorizing payment for fraudulent invoices that billed the foundation for work not performed either by Richardson's shell corporation or other vendors. ([Source](#))

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

Terminated Energy Employee Threatens To Leak Data On 2 Million Customers Because Company Outsourced Jobs Overseas - August 18, 2026

Australian utility Origin Energy is dealing with a serious situation after terminating an employee who is now threatening to release the sensitive personal data of approximately 2 million customers. This Insider Threat incident has triggered a massive federal investigation and exposed critical vulnerabilities in the corporate management of vast consumer databases.

The former employee, who previously possessed authorized access to internal systems, claims the data theft is a direct protest against Origin Energy's policy of outsourcing jobs overseas.

The incident highlights a new twist in how a disgruntled former employee is utilizing stolen customer data, not merely for financial extortion, but for ideological retaliation and corporate blackmail.

The former employee contacted media outlets and Origin Energy management directly in early July 2026, providing a sample of 50 highly detailed customer records to verify they were real. The former employee demanded that the company settle the matter within 14 days, threatening to publish the entire database on the dark web if their demands regarding the cessation of offshore outsourcing were not met.

Origin Energy's internal review currently estimates the breach affects approximately 900,000 current and former customers out of its total 4.8 million account base.

The narrative surrounding the ransom demands has become highly convoluted. Late last month, the employee contacted the press to claim that a private agreement had been reached with Origin Energy and that no data would be leaked. Despite these claims, Origin Energy denied engaging in any financial negotiations or paying a ransom. ([Source](#))

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

No Incidents To Report)

THEFT OF ORGANIZATIONS ASSETS / DESTRUCTION OF PROPERTY

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERNAL OR EXTERNAL ACCOMPLICES)

AT&T Store Worker Sentenced To Prison For Working With Cyber Criminals In Cell Phone SIM Swap Scheme Causing \$593,000+ In Losses To Customers - September 11, 2026

A former AT&T retail worker who used his system access to hijack customers' phone numbers for cybercriminals has been sentenced to 16 months in federal prison.

Kenneth Carter, 44, carried out the SIM swaps at a store in Portland, Oregon, , allowing the criminals to intercept authentication codes and raid victims' bank accounts.

Court documents show that Carter worked with at least three other people in the scheme, which ran between May 2018 and November 2019, and caused nearly \$600,000 in intended losses. Co-conspirator One, described in court documents as the operation's main "hacker," identified victims with online bank accounts, gathered their personal data, and sent it to Carter, who could reassign their phone numbers.

Carter abused his access to AT&T's systems to transfer victims' phone numbers to devices controlled by the other criminals. His role was described as "instrumental to the scheme."

Prosecutors said Carter was paid between \$1,000 and \$2,000 per swap, although he maintained that he earned less than \$4,000 in total.

Law enforcement raided Carter's residence in November 2019, finding copies of the personal data provided to him to carry out the SIM swaps, including the Social Security number of the one victim whose money was successfully stolen. ([Source 1](#)) ([Source 2](#))

2 Office Of Motor Vehicles Employees Convicted In Bribery Scheme Enabling 100+ People To Fraudulently Obtain Commercial Driver's Licenses - September 10, 2026

6 individuals have been convicted in a bribery scheme, that enabled more than 100 people to fraudulently obtain commercial driver's licenses.

Mahmoud Alhattab who is a restaurant owner, led a scheme in which Commercial Driver's License (CDL) applicants paid him an average of \$5,000 to obtain unearned CDLs. The scheme enabled applicants to bypass all three main federally-mandated steps of the CDL qualification process: the knowledge test, entry-level driver training, and the skills test.

To bypass the knowledge test, Alhattab bribed Shakera Millien and Jenay Davis, employees at the Donaldsonville, Louisiana OMV office. Alhattab typically sent Millien and Davis a photograph of an applicant's driver's license via cell phone, along with any requested endorsements, such as a school bus endorsement. Millien and Davis then completed the applicant's knowledge test. They used their cell phones to conduct online research to answer test questions. For example, one on occasion, Millien visited webpages on brake inspection, vehicle fires, hazardous materials, and how to stop a skidding trailer. Similarly, on one occasion, Davis conducted online searches for emergency-controlled braking, hydraulic brake failure, and pre-trip vehicle inspections. ([Source](#))

5 QVC Employees Arrested For Theft Of \$58,000+ From Credit Card Refund Fraud Scheme - August 31, 2026

Five former employees of the digital retailer QVC were arrested and booked into the Florence County Detention Center in South Carolina. Jessica Purvis, Tameka Rogers, Imani Rogers, Yaysher Grice and Jaquanna Davis were charged with breach of trust with fraudulent intent. Local deputies worked alongside QVC's global security operations to uncover a scheme where the employees allegedly manipulated refund credits for purchased goods that were never actually returned, totaling over \$58,000. ([Source](#))

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

No Incidents To Report

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

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

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

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 compiled 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-Public 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 ORGANIZATIONS 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 Fraud 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 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 living 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](#)

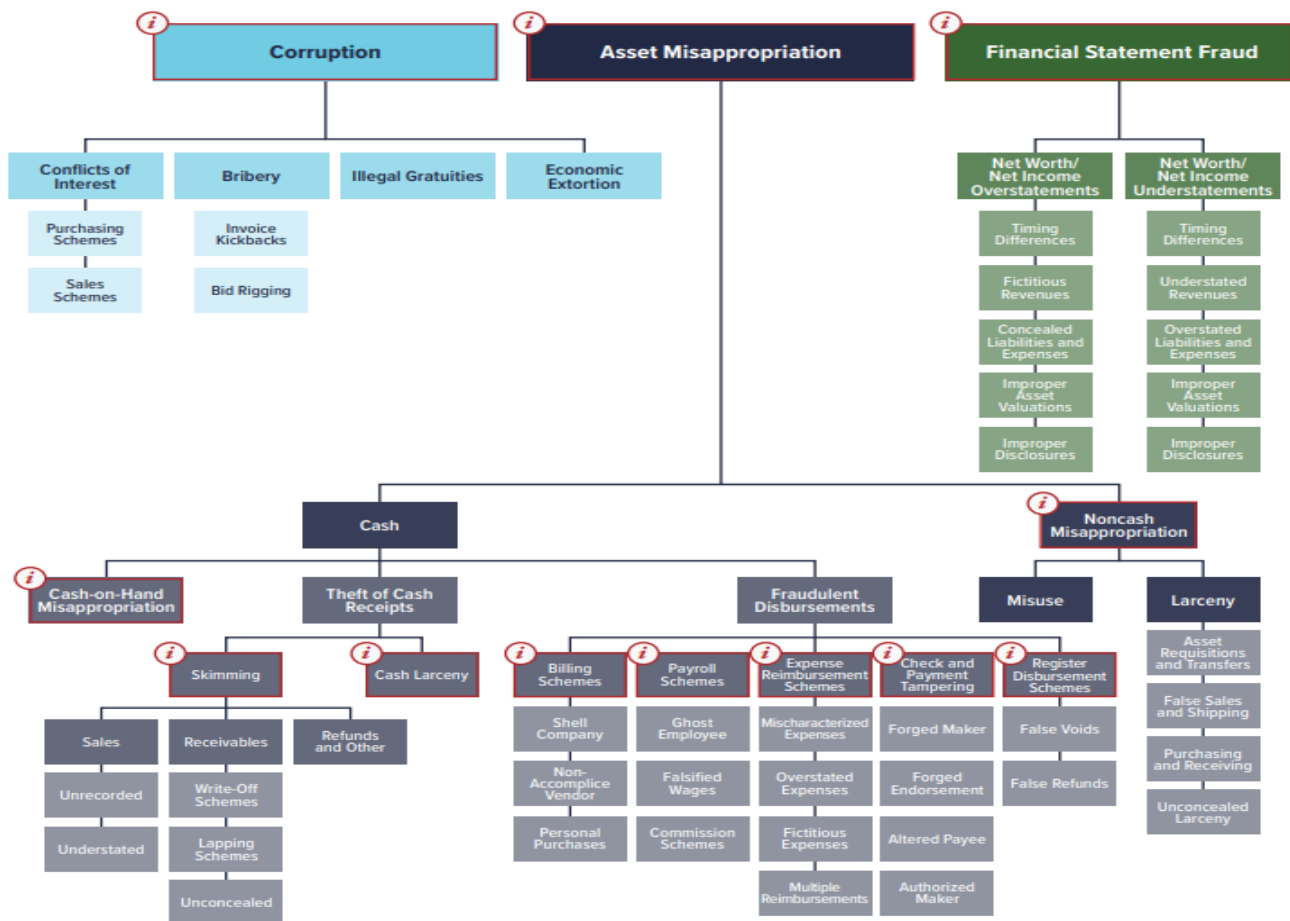
[Fraud Red Flags & Indicators](#)

[Comprehensive List Of Fraud Indicators](#)

THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM

Click on occupational fraud categories below with the ⓘ icon to view definitions and statistical information from the ACFE's *Occupational Fraud 2024: A Report to the Nations*.



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 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 sentenced to 10 years in prison 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 INVOLVED?

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 bank's money to pay Ryan individually or fund Ryan's own businesses. Using bank money this way helped Ryan conceal 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 bank's 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 Brandon 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

Protect America's Competitive Advantage

High-Priority Technologies Identified in China's National Policies

CLEAN ENERGY	BIOTECHNOLOGY	AEROSPACE / DEEP SEA	INFORMATION TECHNOLOGY	MANUFACTURING
CLEAN COAL TECHNOLOGY	AGRICULTURE EQUIPMENT	DEEP SEA EXPLORATION TECHNOLOGY	ARTIFICIAL INTELLIGENCE	ADDITIVE MANUFACTURING
GREEN LOW-CARBON PRODUCTS AND TECHNIQUES	BRAIN SCIENCE	NAVIGATION TECHNOLOGY	CLOUD COMPUTING	ADVANCED MANUFACTURING
HIGH EFFICIENCY ENERGY STORAGE SYSTEMS	GENOMICS	NEXT GENERATION AVIATION EQUIPMENT	INFORMATION SECURITY	GREEN/SUSTAINABLE MANUFACTURING
HYDRO TURBINE TECHNOLOGY	GENETICALLY - MODIFIED SEED TECHNOLOGY	SATELLITE TECHNOLOGY	INTERNET OF THINGS INFRASTRUCTURE	NEW MATERIALS
NEW ENERGY VEHICLES	PRECISION MEDICINE	SPACE AND POLAR EXPLORATION	QUANTUM COMPUTING	SMART MANUFACTURING
NUCLEAR TECHNOLOGY	PHARMACEUTICAL TECHNOLOGY		ROBOTICS	
SMART GRID TECHNOLOGY	REGENERATIVE MEDICINE		SEMICONDUCTOR TECHNOLOGY	
	SYNTHETIC BIOLOGY		TELECOMMS & 5G TECHNOLOGY	

Don't let China use insiders to steal your company's trade secrets or school's research.
The U.S. Government can't solve this problem alone.
All Americans have a role to play in countering this threat.

Learn more about reporting economic espionage at <https://www.fbi.gov/file-repository/economic-espionage-1.pdf/view>
 Contact the FBI at <https://www.fbi.gov/contact-us>






NITSIG INSIDER THREAT SPECIALIZED REPORTS

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

There is NO REGISTRATION required to download the reports.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**7,400+ Incidents**).

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

<https://twitter.com/InsiderThreatDG>

Follow Us On Twitter: [@InsiderThreatDG](https://twitter.com/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 primary focus 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-r8avhdlez>

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 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 **EXCEPTIONAL** 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, Verizon, 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](#)