INSIDER THREAT INCIDENTS REPORT FOR

★ June 2026 ★

DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM

Produced By

National Insider Threat Special Interest Group

★

Insider Threat Defense Group

TABLE OF CONTENTS

INSIDER THREAT INCIDENTS OVERVIEW

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **7,200+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

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

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

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

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

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

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

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

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 26** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR JUNE 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES
No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS
No Incidents To Report

U.S. GOVERNMENT

Security Administration Employee Found Guilty Stealing $1.8 Million+ Of Social Security Funds Over 12 Years - June 25, 2026

Myrna Faria was employed by the Social Security Administration (SSA) from approximately 1991 through 2019 as a Social Insurance Specialis and Claims Specialis" working in the Workload Support Unit in San Juan, Puerto Rico.

From March 2012 through March 2024, Faria embezzled and stole approximately $1,812,455.10 in SSA funds, namely Retirement Insurance Benefits, Survivors Insurance Benefits and Auxiliary Benefit payments, to which she knew she was not entitled.

Faria utilized her position within SSA to submit false claims on behalf of others, using the identity of individuals she believed to be deceased. She then approved those false claims and submitted her own bank and address information to fraudulently receive the corresponding SSA beneficiary proceeds. Faria proceeded to withdraw, transfer, and spend the money from the accounts that fraudulently obtained the SSA funds. Over the span of twelve years, Faria submitted and approved 13 fraudulent claims. (Source)

13 Individuals Charged In $1 Million+ Dollar Bank Fraud Scheme That Involved Bribing U.S. Postal Service Employee - June 25, 2026

Jahquel Robertson, 31, 12 others were charged in April with participation in a large-scale bank fraud scheme involving over $1 million dollars in stolen checks.

According to the indictment, Robertson and the 12 co-conspirator conspired to defraud various businesses, individuals, and financial institutions throughout the United States using stolen, forged and counterfeited financial instruments to fraudulently obtain money under the control of financial institutions.

Robertson received more than $1,000,000 of checks stolen out of the mail by bribing a corrupt United States Postal Service employee. The USPS employee provided Robertson with checks that were originally mailed to or sent by individuals and businesses in the Northern District of New York. Robertson and his coconspirators then used personal identifying information and banking information of willing participants in the scheme to attempt to make fraudulent deposits of checks designed to appear identical to those stolen by the USPS employee. (Source)

Former National Security Advisor John Bolton Pleads Guilty To Retaining & Transmitting Classified Information - June 26, 2026

John Bolton has plead guilty to retaining classified information. Authorities raided Bolton's home and office in August of last year, and he was officially indicted in October 2025. That indictment charged Bolton with both transmission and retention of classified information.

Bolton served as National Security Advisor between April 2018 and September 2019. During this time, Bolton incorporated highly sensitive classified information that he learned from his official duties into personal "diary" entries that he wrote about his daily activities.

These diaries contained information classified up to the TOP SECRET level, as well as Sensitive Compartmented Information. This included foreign adversaries' military operation plans, covert U.S. government actions in foreign countries, and intelligence about adversary foreign leaders obtained from clandestine human sources and intercepted communications.

Bolton sent these documents to two family members who were not authorized to access, receive, or possess classified information. He sent the documents via non-governmental email accounts and a non-governmental messaging application which are not approved for processing classified information. Bolton also retained copies of these documents at his Bethesda home where they were not permitted to be stored.

After Bolton left office in September 2019, a cyber actor, believed to be associated with the Islamic Republic of Iran, hacked Bolton's personal email account. He reported the hack to law enforcement but did not tell the agents, or anyone else in the U.S. government, that the account contained national defense information. (Source)

Former Oak Ridge National Laboratory Employee Sentenced To Prison For Acting As A Foreign Agent - June 18, 2026

In 2023 and 2024, Portia Anyamba worked as a Program Management Operational Specialist in the National Security Program Office at Oak Ridge National Laboratory (ORNL). ORNL is a unique facility located in the Eastern District of Tennessee that was established in 1943 as part of the Manhattan Project and is currently a United States Department of Energy facility dedicated to energy, innovation, and national security, among other things.

During the course of the investigation, FBI agents learned that Anyamba regularly communicated with an intelligence officer working for the Republic of South Africa's State Security Agency (SSA), i.e., the South African Government's civilian intelligence agency.

While under the control of foreign agents, Anyamba was in the midst of her application process for a United States Government security clearance, which, if granted, would have provided her access to certain classified information. Anyamba certified that she had no continuing contact with a foreign national and that she had not had contact with representatives of a foreign government in the past seven years. (Source)

U.S. Agency For International Development Employee Pleads Guilty To Illegally Receiving $176,000+ Of CARES Act Funds / Used Funds For Housing Payments, Etc. - June 3, 2026

A former U.S. Agency for International Development (USAID) employee (Simeon Bakare, 55), pled guilty to charges stemming from a Coronavirus Aid, Relief, and Economic Security (CARES) Act scheme that enabled him to illegally obtain more than $176,000. Bakare previously worked on information technology matters for USAID.

Beginning in April 2020, and continuing until November 2021, Bakare knowingly and willfully engaged in a scheme to defraud the SBA. Bakare admitted he submitted, or caused the submission of, multiple fraudulent PPP and EIDL applications. Additionally, through this scheme, Bakare caused the deposits of EIDL and PPP benefits into bank accounts he controlled.

None of the businesses Bakare listed on the applications had significant employees, office space, revenues, costs of goods sold, or business operations. Bakare admitted he used the PPP and EIDL proceeds for improper personal purposes, such as car and housing payments, along with grocery costs. (Source)

Voice Of America Employee Sentenced To Prison For Threatening To Kill Former Rep. Marjorie Taylor Greene – June 18, 2026

A former Voice of America (VOA) employee was sentenced to prison after he threatened to kill former Rep. Marjorie Taylor Greene, the U.S. Attorney's Office (USAO) for the District of Columbia announced. VOA is funded by the U.S. Government.

The USAO said that 65-year-old Seth Jason of Edgewater, Md., will spend 30 months in prison after a "15-month campaign of intimidation in which he made anonymous death threats" against Greene.

Court documents state that Jason made eight calls between Oct. 11, 2023, and Jan. 21, 2025, to Greene's congressional offices. "Jason made explicit threats involving shooting and murdering Greene, her staff, and her family, including using AK-47s and stockpiled ammunition," the USAO's release said. According to the USAO, he placed all eight calls from inside the Voice of America headquarters in D.C. while he had "a taxpayer-funded job," U.S. Attorney Jeanine Ferris Pirro said. (Source)

DEPARTMENT OF WAR / INTELLIGENCE COMMUNITY

U.S. Army Sergeant Sentenced To Life In Prison For Attempted Murder Of 5 Soldiers & Fiance At Fort Stewart - June 23, 2026

Sgt. Quornelius Radford, 29, was convicted by a military judge last week of attempting to murder five Soldiers and his fiancé. He was sentenced to six consecutive life sentences with the possibility of parole at the conclusion of his trial June 23 at the Fort Stewart Courtroom.

Radford, was an automated logistics sergeant from Jacksonville, Florida. He is assigned to A Company, 703rd Brigade Support Battalion, 2nd Armored Brigade Combat Team, 3rd Infantry Division.

On the morning of August 6, 2025, Radford left his home after an argument with his fiancé and drove to his unit on Fort Stewart with a loaded firearm. Fearing that Radford was suicidal, his fiancé followed him to the installation. After catching up to Radford in the unit's parking lot, his fiancé attempted to calm him down but Radford pulled out the gun and shot him. Radford then proceeded inside the unit's offices where he shot and wounded four Soldiers and attempted to shoot another Soldier but missed.

It was only when members of the unit subdued Radford that the shooting spree ended. Unit members called 911 and the Soldiers held him down until law enforcement arrived at the scene and apprehended Radford. Soldiers with the unit provided first aid to the four wounded Soldiers and Radford's fiancé until Emergency Medical Services arrived. All five shooting victims survived their injuries.

When interviewed by agents with the Department of the Army Criminal Investigation Division, Radford admitted to the shooting. (Source)

U.S. Army Soldier Pleads Guilty To Murder Of Another Soldier - June 11, 2026

Natravien Landry, 27, a former soldier in the U.S. Army National Guard, pled guilty to murder in the death of U.S. Army Sgt. Andre Stewart Jr.of Georgia.

Landry was an Army National Guard soldier assigned to the 1148th Transportation Company at Fort Gordon. He was working with his Guard unit at Fort Gordon early in the morning of Dec. 14, 2024, when he visited an apartment on the installation of a woman with whom Landry shares a child.

After seeing a vehicle parked outside the apartment and suspecting another man was at the residence, Landry walked inside the apartment to a bedroom upstairs and found Stewart and two children. Landry, who was aware Stewart was unarmed, shot him once in chest. Stewart later was pronounced dead in the apartment.

After the shooting, Landry drove away from Fort Gordon and was arrested about three hours later south of Atlanta on Interstate 85 during a traffic stop by the Meriwether County, Georgia, Sheriff's Office. Deputies recovered a 9 mm Glock pistol that testing proved was used in the shooting. (Source)

U.S. Army Recruiter Pleads Guilty To Stealing PII Of U.S. Army Recruits For $266,000 Identity Theft Loan Scheme - June 8, 2026

Jane Crosby, 35, is a former Sergeant First Class in the U.S. Army and U.S. Army Recruiter.

Crosby has pleaded guilty to engaging in a fraudulent scheme to defraud a credit union by using her position to obtain the personally identifying information of U.S. Army recruits and recruit candidates and then submitting fraudulent bank account applications to the credit union on the recruits' behalf.

Between around September 2023 and December 2023, Crosby submitted "Pre-Active Duty Membership" bank account applications to a credit union on behalf of seven U.S. Army recruits or purported recruits, without their knowledge or consent. Such accounts are intended to facilitate the direct deposit of soon-to-be service members' salaries once they join the military. These applications included the victims' names and Social Security numbers as well as copies of their passports, driver's licenses, and/or Social Security cards. Once these credit union accounts were opened, Crosby, posing as the victims, applied for approximately $266,000 in loans and credit card accounts and used the accounts to deposit fraudulent checks and withdraw funds. (Source)

SECURITY CLEARANCE RELATED

Pentagon Legal Opinion Ends DCSA Security Clearance Hearing Program – June 15, 2026

A May 11 legal opinion by T. Elliot Gaiser, assistant attorney general, found that DCSA and other intelligence organizations that conduct supplemental clearance investigations are "investigating entities" under Executive Order 12968. Because the executive order requires individuals facing clearance denial or revocation to appear before an authority other than the investigating entity, Gaiser concluded those organizations are prohibited from conducting the review hearings themselves.

What Clearance Holders Should Know

For clearance holders and applicants, the immediate takeaway is that DCSA personal appearance hearings are suspended, and affected cases are headed to DOHA.

For individuals who received an adverse decision through the DCSA process, the memo creates the possibility of further review if DOHA determines due process was denied.

For agencies, the message is broader. Components that conduct investigations — including supplemental investigations — cannot also conduct the review hearings required under Executive Order 12968.

That could affect more than DCSA. It may require intelligence components and other Department organizations to examine whether their clearance review processes maintain sufficient separation between investigation and adjudicative review. The government still has the authority to deny, revoke, or suspend access to classified information when national security requires it. Nothing in the Matthews memorandum changes that. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 County Sheriff's Office Employees Charged For Embezzling $3 Million+ For Over 20 Years - June 18, 2026

A federal grand jury has returned a five-count indictment charging former employees (Barbara Gooden, 60, and Lisa French, 48) of the Berkeley County Sheriff's Office in West Virginia with conspiracy to commit bank fraud and multiple counts of bank fraud stemming from an alleged long-running scheme to steal taxpayer funds and misappropriate conservator account assets

From 2007 to 2024, Gooden and French conspired to defraud by embezzling cash payments collected by the Sheriff's Office and manipulating conservatorship and estate bank accounts under the office's administration. In carrying out their scheme, defendants issued fraudulent checks, forged signatures, misused a signature stamp, and diverted funds for personal use.

Gooden and French are alleged to have misappropriated more than $3 million. The alleged fraud included fraudulent checks drawn from conservator accounts and issued either to the "Berkeley County Sheriff & Treasurer" or to a private business, to benefit Gooden and French. In total, the defendants allegedly carried out more than 700 fraudulent transactions, including over 550 forged checks, withdrawing substantial funds from at least 59 conservator bank accounts. (Source)

New York City Police Department Detective Sentenced To Prison For $3 Million Paycheck Protection Program Fraud Scheme - June 3, 2026

John Bolden was sentenced to 48 months in prison for wire fraud conspiracy in connection with a scheme to defraud the Paycheck Protection Program (PPP). At the time of his criminal conduct, Bolden was a detective with the New York City Police Department (NYPD). In addition to the prison term the judge ordered Bolden to pay restitution in the amount of $303,138 and forfeiture in the amount of $112,002.

Then-detective Bolden owned partnership interests in a franchise for a tax-preparation business. Between May 2020 and October 2022, Bolden engaged in a scheme to defraud the Small Business Administration by working with his clients to fraudulently obtain PPP funds.

Bolden obtained PPP funds for himself, his co-defendants and more than 65 individuals by helping submit online loan applications containing false and fraudulent information. One of those loan applications belonged to co-defendant Anthony Carreira, also a former NYPD detective, who knowingly submitted false documentation to obtain PPP funds. Co-defendant Christian McKenzie, who is Bolden's cousin, also fraudulently obtained a PPP loan and steered other applicants to Bolden in exchange for fraudulent PPP proceeds. As part of the scheme, Bolden prepared fictitious Internal Revenue Service Form Schedule C documentation, which accompanied the loan applications and contained false information about his, his co-defendants' and his clients' places of employment, gross income and net income. Bolden sought to steal nearly $3 million from the PPP, and succeeded in stealing at least several hundred thousand dollars. (Source)

New York City Department Of Corrections Captain Charged For $650,000+ Of Wage Fraud & Extortion Of Co-Workers - June 11, 2026

Latanya Brown has been employed by the DOC since October 2001 and has held the rank of Captain since July 2007. Between approximately July 2024 and November 2025, Brown was assigned to Rikers Island's Facility Operations Department as a DOC supervisor. Between approximately November 2025 and December 2025, Brown was assigned to New York State courthouses located in the Bronx.

As a Captain, Brown supervised other correction officers and was responsible for approving employee requests for shift-schedule changes, overtime shifts, and vacation time.

In 2024 and 2025, Brown regularly threatened to withhold approvals for shift changes, overtime shifts, and vacation time requests for her officers unless they agreed to pay her money, buy luxury items for her, and / or perform personal errands for her. For example, in December 2024, Brown forced several officers to buy an expensive Louis Vuitton bag for her. When Brown made her demand, she made statements to the DOC officers implying, in sum and substance, that their shift assignments, overtime shifts, and vacation time would be in jeopardy unless they purchased the luxury item. Additionally, on numerous occasions, Brown forced officers to drive her while on duty for non-work-related purposes, such as visits to restaurants, bars, and a casino.

In 2024 and 2025, Brown received more than $250,000 in regular pay and more than $400,000 in overtime pay. However, on more than 100 occasions during this time period, Brown submitted documentation to the DOC claiming that she had worked the entirety of regular and overtime shifts, when in fact she actually arrived to work several hours late or left work several hours early on those occasions. On some occasions, when Brown left her assigned posting early, she did so to spend time at the Empire City Casino in Yonkers, New York. For example, on November 21, 2024, Brown claimed in documentation submitted to the DOC to have worked from 5:00 a.m. until 9:31 p.m. on Rikers Island. However, Brown was not at Rikers Island during the entirety of that shift and instead arrived at the casino that day at approximately 2:34 p.m. Nevertheless, Brown was compensated by the DOC as if she had worked her full shift and at least seven hours of overtime. (Source)

New York City Department Officer Sentenced To Prison For Accepting $30,000+ In Bribe Payments & Distributing Narcotics - June 22, 2026

Andrew Nguyen is a former officer in the New York City Police Department (NYPD)

From approximately 2020 to 2023, Nguyen used his position as a police officer in the NYPD to solicit and accept tens of thousands of dollars in bribe payments in exchange for assisting another individual with the operation of drug trafficking enterprise. Nguyen accepted $30,000+ in bribe payments from the individual running the drug trafficking enterprise (and solicited tens of thousands of dollars in additional bribes) in connection with Nguyen's participation in the drug trafficking enterprise. (Source)

Police Officer Found Guilty For Fraudulently Obtaining $18,000+ Of COVID Paycheck Loans / Used Funds For Gambling - June 8, 2026

Roberto Adams, 39, is a former Metropolitan Police Department officer residing in Hyattsville, Maryland. He was found guilty today in connection with a scheme to fraudulently obtain more than $18,000 in COVID Paycheck Protection Program loans.

Adams obtained Paycheck Protection Program loans on behalf of his business SuperKlean LLC, a janitorial services company that was not operational at the start of the pandemic. He obtained a first PPP loan in July 2020 and spent those funds in approximately one month at casinos in Maryland and Las Vegas, on airfare and hotels in Miami, at restaurant and bars, and on hangover treatments.

On Jan. 21, 2021, Adams applied for a second PPP loan. Eight days later, on Jan. 29, 2021, $18,345, representing the second draw of the PPP loan funds, was deposited into Adams' checking account.

He quickly spent those funds paying off personal debts, including over $12,000 in back rent as well as other personal extravagances such as clothing and high-end sneakers.

In April 2021, Adams applied for a job with the Seattle Police Department. In the course of his background check, a Seattle Police Department detective noticed that Adams had obtained a PPP loan but had failed to disclose it in his written application or during an interview with the detective, as required. When confronted, Adams falsely claimed that the "purpose of the loan was to provide relief and assistance for my small business during the pandemic." (Source)

Bureau Of Prisons Contractor Employee Charged With Accepting $163,000+ In Bribes To Smuggle Contraband Into Prison - June 24, 2025

From January 2024 through August 2025, Terri Outer was employed as a contractor at FCI Otisville, in New York, working as a dental assistant.

During her time there, Outer solicited and received payments in return for smuggling contraband and prohibited objects into the prison. Outer received more than $163,000 from inmates' family members and associates, and engaged in extensive communications with inmates, former inmates, and their family members and associates, including discussions with an inmate about having the contents of a package weighing over six pounds smuggled into FCI Otisville. (Source)

Federal Correctional Officer Sentenced To Prison For Accepting $43,000+ In Bribes To Smuggle Contraband Into Prison - June 1, 2026

Karen Torres, 50, was a public official employed by the U.S. Department of Justice, Federal Bureau of Prisons, as a correctional officer. She worked at the Coleman Federal Correctional Complex (FCC Coleman) in Sumter County. Between May 2022 and March 3, 2025, Torres introduced contraband (marijuana, cigarettes, and K2) into FCC Coleman in exchange for $43,550 in bribes from inmates. (Source)

County Corrections Officer Sentenced To Prison For $54,000+ COVID Unemployment Loan Fraud Scheme - May 28, 2026

A former Suffolk County Sherriff's Department Corrections Officer (Christnel Orisca, 26) in Boston, was sentenced in federal court for submitting fraudulent information in order to obtain loans through CARES Act programs like the Pandemic Unemployment Assistance (PUA) program and the Paycheck Protection Program (PPP). Orisca was a corrections officer with the Suffolk County Sherriff's Department from late 2021 to December 2024.

Orisca fraudulently applied for pandemic unemployment and small business loan benefits while working full-time, initially for a security company and later for a delivery company. While employed full-time, Orisca collected approximately $54,700 in unemployment benefits and small business loan funds. (Source)

Employee Working At Jail Handling Financial Matters Sentenced To Prison For Stealing $21,000+ - May 28, 2026

Pamela McDonald, 41, worked as the "jail matron" at the Starke County Jail in Indiana.

Her duties included paying invoices with funds from the jail commissary account. She devised a scheme to unjustly enrich herself by depositing commissary funds into her personal PayPal account while camouflaging the transfers as payments for legitimate invoices. Between August 15, 2022, and May 15, 2023, McDonald made at least 19 unauthorized withdrawals and pocketed at least $20,621.85 that she was not entitled to receive. She also used a Starke County debit card to purchase a video gaming chair, a memory foam mattress, and a full-size bed frame for her home totaling $658.57, resulting in a total loss to Starke County of $21,280.42. (Source)

LAW FIRMS

Law Firm Paralegal Charged With Embezzling $460,000+ From Firm - June 12, 2025

From May 2024 to March 2025, Yelena Andrews, 48, while employed as a paralegal with an Erie, Pennsylvania, law firm, devised a scheme steal from the law firms. Andrew's actions resulted in the embezzlement of approximately $462,376 to which she was not entitled. (Source)

Law Firm Employee Charged With Embezzling $115,000 From Firm - June 22, 2026

Tonya Hallmark, 59, is facing theft charges after authorities say she embezzled nearly $115,000 from a law office over a two-year period. Hallmark worked for attorney James Allison Jr., managing his law office's finances. Douglas County sheriff's investigators allege she stole $114,866 between April 1, 2024, and March 1, 2026. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Hawaii County Housing Official Sentenced To Prison For His Role In $11 Million+ Scheme To Receive Bribes From Businessman & Attorneys - May 29, 2026

Paul Sulla, 79, and Gary Zamber, 56, both attorneys living in Hawaii, and Rajesh Budhabhatti, 65, a private businessman living in Hawaii. conspired to pay bribes and kickbacks to Scott Rudo, 59, in exchange for Rudo's agreement to use his official position to ensure the county approved three affordable housing agreements (AHAs) benefitting the defendants' development companies, Luna Loa Developments LLC, West View Developments LLC and Plumeria at Waikoloa LLC.

Although Rudo's co-conspirators promised in the AHAs to build affordable housing for the citizens of Hawaii County, their development companies never built a single unit. Through the AHAs, the defendants fraudulently obtained more than $11 million worth of land and excess affordable housing credits (AHCs). From that amount, Sulla, Zamber, and Budhabhatti paid or attempted to pay Rudo approximately $1,931,778 in bribes and kickbacks. (Source)

City Employee Pleads Guilty To Helping Embezzle & Launder $1.5 Million Of City Funds / Used Funds To Pay Personal Credit Card, Wedding Reception, Etc. - May 29, 2026

From 2010 until 2022, Roberta Shaffer, 61, was employed as assistant to the City Manager of DuBois, in Pennsylvania. The city which received federal assistance through grants, subsidies, loans, guarantees, insurance, and other forms in excess of $10,000 in each of the calendar years from 2008 to 2022. In her role as assistant, Shaffer and then-City Manager John Suplizio opened four secret bank accounts that were neither approved nor signed for by the appropriate city officials as required under Pennsylvania law, with Shaffer instead signing the account opening documents at Suplizio's direction.

Suplizio then diverted approximately $1.5 million that should have been deposited into accounts controlled by the city into the secret accounts, from which Suplizio used the stolen money to make payments on his personal credit card and to pay for various personal expenses, as well as for substantial cash withdrawals made for Suplizio's benefit. Shaffer wrote and signed many of the checks that paid for the credit card bills and resulted in the cash withdrawals. The secret accounts were also used to pay for donations to local politicians, a fundraiser dinner for a local judge, and a city employee's wedding reception. In addition, several cashier's checks purchased through withdrawals from the secret accounts, as well as numerous large cash deposits, were later deposited into Suplizio's personal banking accounts. (Source)

Director For Chicago Housing Authority Charged For Accepting $421,000+ In Kickback For $4.8 Million+ In Construction Contracts - June 9, 2026

Ryan Ross is the former property director for the Chicago Housing Authority (CHA).

Ross was given more than $421,000 in kickbacks from the owner of a construction company in exchange for steering that owner more than $4.8 million in construction and renovation work at CHA properties.

Ross received the kickbacks in 2023 and 2024 from Vanessa Rhodes, the President of Bell's Better Buildings, Inc., a Chicago company that did business as Twenty Eleven Construction, Inc. In exchange for the kickbacks, Ross used his official position as a Director at the CHA to fraudulently award construction, renovation, and other work to Twenty Eleven Construction and another company affiliated with Rhodes. As part of the scheme, Ross and Rhodes also caused Rhodes's husband to falsely represent himself to CHA property managers as an employee of the affiliated company who would purportedly complete the work on CHA units. (Source)

Director For Newark, NJ Department Economic & Housing Development Sentenced To Prison For Accepting $25,000 In Bribes - June 3, 20276

From at least 2017 through April 2019, while serving as a high-level Newark official, and prior to that, as an executive officer of the NCEDC (now known as Invest Newark), Carmelo Garcia sought and received significant monetary payments and other benefits from Frank Valvano, Irwin Sablosky and others in exchange for Garcia's use of his official positions and influence within the City of Newark and the NCEDC to advance real estate development matters of interest to Valvano and Sablosky. These matters included obtaining preliminary designation letters for Valvano and Sablosky and securing Newark-approved redevelopment agreements (RDAs) that allowed them to purchase and acquire various Newark-owned properties for redevelopment, and to ensure that Garcia did not use his influence and authority to act against their interests.

Phone records and text messages obtained by law enforcement show extensive communication between Garcia, Valvano, Sablosky, and others throughout this period of time, including text messages in which Garcia arranged to personally collect cash provided by Valvano and Sablosky.

In one instance, in June 2018, Garcia, then the City's Acting Deputy Mayor and Director of the City's DEHD, received an envelope containing $25,000 in cash, supplied by Valvano through an intermediary, in the restroom of a New Jersey restaurant. In addition to cash, Garcia also received jewelry, including multiple high-end watches and chains, from Valvano and Sablosky's pawnbroker and jewelry business. (Source)

County Social Services Employee Sentenced To Prison For Stealing $100,000 - June 25, 2026

Deshaune White, was sentenced to 6 months years in federal prison and 6 months home confinement, followed by 3 years of supervised release for his role in a scheme to defraud more than $100k in Supplemental Nutrition Assistance Program (SNAP) benefits administered by the United States Department of Agriculture (USDA) and managed by the North Carolina Department of Health and Human Services, and county Division of Social Services (DSS).

White, using his position and privileges as a Lenoir County Social Services case worker, unlawfully accessed the SNAP accounts of qualified individuals and converted $102,733.80 in government funds for his own personal benefit and use. (Source)

State Court Clerk Charged For Embezzling $44,000+ / Used Funds For Personal Expenses Such As Bars, Hotels, Restaurants, Etc. - June 15, 2026

A federal grand jury has returned a six-count indictment in a significant public corruption case against that involved Tennessee Shelby County General Sessions Court Clerk Tamara Sawyer.

Between August 2024 and June 2025, Sawyer embezzled $44,607.35 in public funds to her own use. She carried out the scheme by using procurement cards issued to other county employees, a county travel card, and by obtaining travel advances.

Sawyer used these cards to pay for a wide range of personal expenses for herself and others, including alcohol, food and goods ordered through web-based delivery services such as Uber Eats and Instacart, as well as charges at bars, hotels, restaurants, the Memphis Tigers, FedEx Forum, Turo, local fundraisers, and payments to various PayPal accounts—including her own.

Many of these transactions occurred on weekends or holidays when the clerk's office was closed. Although Sawyer claimed the expenses were for official business, the investigation determined they were personal in nature.

Sawyer also used the procurement cards as part of a money-laundering scheme. She transferred stolen funds to a PayPal account controlled by a friend, who kept a small portion and returned the remainder to Sawyer through CashApp. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Bus Driver Sentenced To Prison For Setting Bus On Fire That Had 42 Children On Board - June 2, 2026

Michael Ford is a former Granite School District Bus Driver in Utah. According to court documents and admissions made at Ford's change of plea and sentencing hearings, he intentionally set a Granite School District school bus on fire with a cigarette lighter on April 7, 2023.

Ford was captured on video igniting the bus and continued to drive the bus with smoke billowing past his face. In other court documents, prosecutors stated that Ford attempted to tamper with the bus's video surveillance system in the days preceding the April 2023 arson.

On a separate occasion in February 2022, Ford was also accused of setting a Granite School District school bus on fire that had 42 children inside and did so while driving in traffic, but the charge was dismissed as part of his plea agreement. (Source)

3 School Employees Sentenced To Prison For Embezzling Nearly $400,000 Of Federal Program Funds - June 2, 2026

Mario Willis was the superintendent of Hollandale School District. From July 2019 to May 2022, Joe Nelson was the superintendent of Clarksdale Municipal School District. In October 2022, Nelson became the superintendent of Leake County School District.

Monekea Smith-Taylor was a schoolteacher in the St. Louis, Missouri area. Nelson and Willis used their position as school superintendents to commit the crimes and, together with Smith, embezzled public funds for their own enrichment. (Source)

Business Administrator For School District Charged For $70,000 Overtime Fraud & Kickback Scheme - June 3, 2026

A federal grand jury returned an indictment charging the former Business Administrator (Aiman Mahmoud, 56) of the Hillsborough Township School District (HTSD) with an overtime fraud and kickback scheme.

Mahmoud served as the Business Administrator for the HTSD from 2008 through the end of 2021. Mahmoud accepted tens of thousands of dollars in cash kickbacks in connection with a multi-million dollar project that aimed to upgrade existing school facilities as well as to construct a new school building that had been greenlighted by a 2019 referendum. To oversee aspects of the project including safety monitoring, Mahmoud arranged for Kenneth Gratto, 54, to be appointed as the site supervisor / owner's representative to assist two companies involved in carrying out the construction project.

Shortly after Gratto was hired, Gratto agreed to provide substantial cash kickbacks to Mahmoud in exchange for Mahmoud's agreement to approve Gratto's time sheets which substantially exaggerated the number of overtime hours that Gratto had worked on behalf of the HTSD.

After receiving his paychecks from the companies involved – who were in turn reimbursed by the HTSD for those amounts – Gratto would deposit the checks, withdraw cash in the amount of the intended kickback, and deliver that cash in envelopes at locations of Mahmoud's choosing, typically, within Mahmoud's unlocked school vehicle. Mahmoud is alleged to have taken at least approximately $70,000 in kickbacks from Gratto. (Source)

School Employee Charged With Embezzling $40,000+ June 5. 2026

Detectives from the Financial Crimes Unit have charged a Fairfax County Public Schools (FCPS) Finance Technician with Embezzlement and Computer Fraud.

On April 21, 2026 detectives launched an investigation after receiving information from the FCPS Auditor General of potential misappropriation of funds by an employee at Hayfield Secondary School. After a thorough investigation, detectives determined that Stephanie Gale, 45, had embezzled over $40,000 from the school. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Church Employee Sentenced To Prison For Embezzling $445,000+ From Church / / Used Funds For Personal Enrichment - June 18, 2026

Shelley Strickland, 55, was arrested by the South Carolina Department of Revenue in March 2026 after it was determined during an investigation she embezzled more than $445,000 from First Baptist Church of Ware Shoals and converted it for personal use. She was employed with the church from 2018 to 2024, officials said. (Source)

Church Employee Sentenced To Prison For Embezzling $410,000+ Of Church Funds - June 26, 2026

Shenia Watson was an employee of Perfecting Church in Toledo, Ohio. Watson was responsible for managing parishioner donations.

Investigators discovered that from about June 2019, to June of 2023, Watson used her position at the church to embezzle church funds from an app that was used to receive donations from parishioners. To conceal her embezzlement activities, Watson knowingly provided the board of directors with fraudulent monthly financial summary reports. Additionally, Watson secured a credit card in the name of the church's pastor and used it to pay church expenses to conceal its true financial condition and to conceal her embezzlement activities. Watson to serve three years of supervised release and pay $410,574.39 in restitution. (Source)

LABOR UNIONS

Union President, His Wife, Union Vice President & Union Treasurer Convicted For Embezzling $7 Million For 15+ Years / Used Funds For Lavish International Travel - June 5, 2026

A federal jury convicted a North Carolina couple, a Missouri man, and an Ohio man in relation to a scheme involving theft of union-member dues through the award of no-show jobs, lavish travels and dinners charged to the union, unearned vacation payouts, and an unauthorized $7 million loan made to a union-related bank.

The jury convicted Newton Jones, 72, the former President of the International Brotherhood of Boilermakers, Iron Ship Builders, Forgers, and Helpers (Boilermakers Union), his wife Kateryna Jones, 33, and the former Secretary Treasurer, William Creeden, 78, of violation of the Racketeering Influenced Corrupt Organization (RICO) Act.

Those defendants, as well as one of the Boilermaker Union's former Vice Presidents, Lawrence McManamon, 78, were convicted of embezzlement from the Union through various means.

Over A 15 Year Period Newton Jones & Willion Creeden Embezzled The Funds For:

- $5 Million+ in unnecessary luxury international travel.
- Nearly $2 Million in salary and benefits to Kateryna Jones and others for no-show jobs, at which they were not required to work, including payment of two years of salary to Kateryna Jones for a period when she resided in Ukraine and was dating Newton Jones.
- Over $100,000 in tuition, rent, and relocation expenses for members of the family of Newton Jones.
- Hundreds of thousands of dollars in cash payments relating to fraudulently claimed vacation time.
- Over $100,000 in restaurant charges by Newton Jones and Kateryna Jones in their hometown.
- Money spent in unauthorized email surveillance of union employees to defend Newton Jones and McManamon from internal union charges.
- $7 Million in unauthorized loans from the Boilermakers Union to the bank at which Newton Jones and Creeden had supposed full-time jobs that required little work and were each paid nearly $500,000 per year while they were also being paid a full-time salary from the union. (Source)

New York County Sheriff's Union Treasurer Charged With Stealing $100,000 From Union / Used Funds For Personal Enrichment - June 22, 2026

Andrew Wells, 42, was arrested and arraigned on a second-degree grand larceny charge, property value exceeding $50,000, the New York State Police said.

Wells was the treasurer of the Ulster County sheriff's union. State Police arrested Wells after the Ulster County Sheriff's Employee Association (UCSEA) found suspicious activity involving its bank account, which set off an investigation launched by the State Police. The probe showed Wells stole approximately $99,418.23 from the UCSEA and used the funds between February 2023 and April 2026, State Police said. (Source)

BANKING / FINANCIAL INSTITUTIONS

Bank Manager Charged With Embezzling $1.9 Million From Bank - May 28, 2026

Heather Casas, 44, has been charged with bank theft, embezzlement, or misapplication by a bank officer or employee. From August 2024 through December 2024, Casas, while working as a bank manager for a bank in Coos Bay, Oregon stole approximately $1.9 million from the bank. (Source)

Bank Branch Manager Sentenced To Prison For Embezzling $800,000+ / Used Funds Lost Engaging In Foreign Currency Trading - June 1, 2026

Tamim Haidar, 34, admitted to abusing his position as an assistant branch manager of a Wells Fargo branch bank to embezzle more than $800,000 from the bank.

Haidar admitted that he would steal money that was supposed to be deposited into ATM machines, and that he made false database entries to hide his theft. Haidar admitted that he transferred the money he stole to his personal bank accounts, and used the stolen funds to make up losses he incurred engaging in foreign currency trading. (Source)

Bank Branch Manager Sentenced To Prison For Role In Embezzling $655,000+ From Bank / Deposited Funds Into Personal Bank Account - June 19, 2026

Brooke McDonough served as the branch manager of a Mesa bank, in Arizona.

McDonough embezzled $655,000 from the bank she managed over the course of 7 months. Between June 2021 and February 2022, McDonough stole cash from the ATMs and vault inside the branch. She also manipulated monthly audits by entering inflated figures into the bank's systems to conceal the increasing cash shortage. The scheme came to light only after McDonough resigned. The discovery of the theft triggered an internal investigation that caused three other bank employees to be placed on administrative leave.

A federal investigation revealed that McDonough deposited most of the cash she stole into her personal bank accounts. She used different ATMs at multiple bank branches breaking deposits into smaller amounts to avoid mandatory Currency Transaction Reports for deposits of over $10,000 in cash. (Source)

Bank Manager Sentenced To Prison For Embezzling $395,000 Over 12 Years - May 28, 2026

Sandra Campfield, 68, was sentenced to prison and a ordered to pay a $50,000 fine for embezzling money by a bank employee. Campfield was ordered to pay $395,103.67 in restitution to the victims of her embezzlement.

Campfield previously worked as the long-time branch manager of a bank in Elroy, Wisconsin. Between September 2012 and August 2024, she used her position at the bank to steal approximately $351,344 from customer accounts. Campfield also took approximately $43,758 worth of foreign currency from the bank's vault. (Source)

TD Bank Employee Pleads Guilty To Receiving $155,000 In Bribes To Facilitate $3.4 Million+ Fraud Schemes At 2 Financial Institutions - May 28, 2026

A New York-based former employee of TD Bank, Cheungkin Lam, pleaded guilty to defrauding TD Bank customers and bribing an employee at another financial institution to falsify bank records, which, in total, facilitated more than $3.4 million of fraud.

From January 2021 through May 2021, Lam accepted bribes and leveraged his position at TD Bank to identify bank accounts with large balances and steal confidential customer information. Lam shared that information with outside co-conspirators, who used it to defraud customer accounts.

Separately, from May 2022 through August 2022, Lam engaged in a scheme to bribe a co-conspirator employed at another financial institution to falsify bank records in opening a bank account for use in various fraud schemes by Lam's co-conspirators. In total, Lam received at least $155,000 in bribes and facilitated $3,433,989.07 in fraud losses. (Source)

TD Bank Employee Sentenced To Prison For Accepting $6,000+ In Bribes For $5.5 Million Money Laundering Scheme To Colombia - June 10, 2026

Leonardo Ayala, 26, accepted bribes and exploited his position as a bank employee to help launder drug money to Colombia.

From June to November. 2023, Ayala opened fraudulent accounts, issued over 150 debit cards to shell companies, and unblocked debit cards that TD Bank had restricted due to questionable activity. The bank accounts and debit cards were then used to make more than 12,000 ATM withdrawals in Colombia, funneling approximately $5.5 million out of the United States. In exchange, Ayala received more than $6,000 in bribes paid in cash and through a peer-to-peer digital payment network. (Source)

Employee At Financial Institution Sentenced To Prison For Stealing $168,000 - June 5, 2026

Between September 2021 and February 2022, Michael Torres, 38, was employed as a Relationship Manager at Financial Institution.

While in this position, he misused his position to apply for loans through financial institution in the names of individuals without their knowledge or authorization. Torres applied for 19 loans for a total of $168,000, which was deposited into bank accounts that he controlled. (Source)

Bank Teller Charged With Stealing $28,000 From Customer Accounts - June 3, 2026

According to a St. Louis County Police Department, Deshauna Lorick worked as a teller at Royal Banks. Between July 14 and Aug. 16, 2023, police said Lorick took screenshots of checks being deposited by 13 customers and sent them to an accomplice in exchange for payments through Cash App.

The screenshots contained customers' names, addresses, phone numbers, account numbers, routing numbers, and check numbers. The accomplice then used that information to fraudulently obtain approximately $28,000 from customer accounts. The bank later detected and stopped an additional $150,000 in fraudulent transactions linked to the stolen information. Lorick was issued a criminal summons and ordered to appear in court on July 13, 2026. (Source)

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

Office Manager For Physical Therapy Clinics Convicted Of $8 Million Medicare Fraud Scheme - May 28, 2026

Olga Popovych was convicted by a federal jury in Brooklyn for her role in an $8 million health care fraud conspiracy.

Popovych was an office manager of several physical therapy clinics in Brooklyn that paid cash kickbacks to ambulette drivers who recruited Medicare patients to transport to clinics.

Popovych was personally involved with paying ambulette drivers cash kickbacks. She also falsified medical records to indicate that physical therapists who were not actually at the clinic treated the patients. Between 2018 and 2020, Medicare paid these clinics over $8 million.

There was witness testimony that Popovych exchanged text messages with her co-conspirators that discussed the payment of kickbacks through the use of code words. The evidence also showed that Popovych suspected that the clinics were being watched by law enforcement and took steps to conceal the scheme. (Source)

Bookkeeper For Physician's Office Sentenced To Prison For Stealing $928,000+ Over 7 Years - June 2, 2026

Bobbie Margiotta, 65, worked as bookkeeper for a physician located in Hancock County, Mississippi. Over the course of nearly seven years, Margiotta stole $928,988.37 from the physician and his companies. Part of her scheme involved the use of interstate wires. (Source)

Employee Working At Assisted Living Facility Charged With Stealing $573,000+ - June 8, 2026

Ezriel Green, 41, was employed by an assisted living facility in Mohawk, New York to manage the facility's finances.

Between October 2024 and April of 2025, Green obtained and cashed over $573,000.00 of checks made payable to the facility and issued by the United States Treasury Department and New York Medicaid. Although these funds were intended for the operation of the facility and the care of its elderly residents, Green cashed the checks and converted the funds to his own use. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Financial Trade Facing Criminal Charge For Stealing Source Code Worth $1 BILLION To Build His Own Company - June 1, 2026

A former quantitative trader at Headlands Technologies has been indicted for allegedly walking out the door with source code worth over $1 billion, then using it to build his own trading startup. If convicted, he faces up to 10 years in prison.

Headlands Technologies spent years developing proprietary components known internally as "Atoms" and "Alphas." Atoms are the building blocks of their trading infrastructure, and Alphas are the predictive algorithms that actually make money.

Ho worked at Headlands as a developer and trader from 2019 to 2021. In spring 2021, while still employed at Headlands, Ho allegedly began developing his own trading firm called One R Squared, or ORS. The indictment claims he misappropriated critical components of Headlands' proprietary code to build it.

Cheuk Fung Richard Ho, 36, was arrested on January 8, 2025, in Los Angeles. He faces one count of theft and attempted theft of trade secrets, brought by the US Attorney's Office for the Southern District of New York. The case was built by the Complex Frauds and Cybercrime Unit with FBI involvement. (Source)

Mortgage Company Suing Competitors & 31 Former Employees For Stealing Trade Secrets - June 12, 2026

OneTrust Home Loans is suing competitors E Mortgage Capital (EMC) and United Wholesale Mortgage (UWM), along with 31 former employees of a former Arizona division, alleging a coordinated scheme to poach staff, steal trade secrets and divert more than $31 million in loan volume.

The complaint by OneTrust — a d/b/a for CalCon Mutual Mortgage — accuses the defendants of secretly funneling borrower information and loan opportunities to EMC and UWM while still employed by OneTrust.

The lawsuit, filed June 4 in a U.S. district court in Arizona, alleges that the defendants "improperly obtained and exploited the benefit of CalCon's employees, borrower information, loan opportunities, confidential information, trade secrets, goodwill and business infrastructure for Defendants' own financial gain."

As of March 12, 2024, the departing group had successfully solicited at least 79 loans away from OneTrust, representing an aggregate loan volume of just over $31 million, the lawsuit shows." (Source)

Senior Level Manager Sentenced To Prison For Stealing Employers Trade Secrets - June 23, 2026 Gy

Guy Galanti, 48, worked as a senior level manager for Green Technology Investments (GTI) in Scottsdale, Arizona. GTI is based in Arizona and is in the business of servicing semiconductor testing machines and selling remanufactured semiconductor testing machines with new functionalities designed by GTI.

Beginning sometime in early January 2025, and continuing to August 2025, Galanti conspired with another individual to steal GTI's newly created Glass Detect Design, which would allow a semiconductor testing machine to locate microscopic defects on a semiconductor wafer made of glass instead of silicon material. Galanti's co-conspirator sought to recreate GTI's new design as he operated a Taiwanese company that directly competed with GTI.

Over the course of several months, Galanti secretly sent photos of GTI's Glass Detect Design, information, and software, to his co-conspirator in an effort to recreate GTI's proprietary system. To conceal their interactions, Galanti and his co-conspirator communicated over an encrypted messaging system, deleted emails and transaction data sent from Galanti's work email, and created fictitious invoices to document the transfer and potential payment of funds to Galanti. (Source)

LastPass Password Management Vendor Data Breach - June 2026

On June 12, 2026 LastPass was made aware of an incident that occurred at Klue (klue.com), a third-party market intelligence platform utilized by our go-to-market teams which integrates with our Salesforce and Gong systems.

The incident had a broad impact across many companies including LastPass. We immediately launched an investigation and learned that, as part of this incident, an unauthorized actor was able to obtain OAuth tokens Klue held for many of its customers, including LastPass. The threat actor then used these credentials to access LastPass customer data within our Salesforce environment. Remediation has been completed, and the exposed Klue OAuth tokens have since been rotated.

The information accessed was limited to standard business contact information and related customer relationship management (CRM) data, including customer names, phone numbers, email addresses, and physical addresses, as well as support case data and sales-related data. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

Hackers Simply Asked Meta AI To Give Them Access To High-Profile Instagram Accounts, And It Worked - June 2, 2026

Hackers say that they used Meta's AI support chatbot to break into a host of high-profile Instagram profiles by asking the support bot to change the email address associated with the target account. The claims coincide with a series of high-profile Instagram account takeovers, including the Barack Obama White House account, the Chief Master Sergeant of Space Force's account, and Sephora's account.

The news shows the extreme risk associated with offloading support or critical functions to an AI chatbot. Users who have had their accounts stolen say that there is no way to escalate their problem to a human.

In March, Meta announced that it was pushing AI support to all accounts across Facebook and Instagram, and that it would have the ability to reset passwords and perform other critical account maintenance functions: "Solutions, not just suggestions," the feature's product page says. "Account security and recovery." (Source)

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

Justice Department, FBI Disable 13 Websites Backed By Suspected Chinese Agents That Sought Sensitive U.S. Information From Security Clearance Holders - June 10, 2026

Beginning in November 2023, the conspirators created at least 13 fake consulting company websites. The websites and their associated job postings advertised generic "consulting" jobs and included statements indicating their purpose was to recruit current or former U.S. government and U.S. military employees to provide expertise to unspecified clients. The websites were typically linked or referenced within the entities' job postings on hiring platforms.

The methods and means used by the conspirators include (1) the use of aliases, fictitious personas, and the stolen identities of actual persons; (2) the use of Artificial Intelligence (AI)-generated photographs; (3) relatively large payments for research reports; (4) the use of Telegram and other encrypted applications; (5) pressure to provide "exclusive" or "insider" information; and (6) the transfer of money from places and accounts located overseas to places and accounts located in the United States.

According to court documents, the conspirators recruited applicants through job postings, on social media and other platforms including Upwork, Expertia AI, Hubstaff Talent, Wellfound, and Post Job Free. The postings related to topics of interest to the government of the People's Republic of China. (Additional Details)

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

No Incidents To Report

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

Non-Profit Executive Director Sentenced To Prison For Embezzling $1.7 Million+ - June 4, 2026

An investigation revealed that during her tenure as Executive Director of the American Indian Center of Arkansas (AICA), Star Jackson completed a withdrawal of funds on approximately June 24, 2024, from the Department of Education grant in the amount of $30,000. The grant funds were deposited into an account opened by Jackson and without the knowledge of AICA's Board of Directors.

On or about June 27, 2024, Jackson completed another withdrawal of funds from a Department of Health and Human Services grant in the amount of $40,000.

Those grant funds were deposited into a non-active AICA account that Jackson still had access to, along with grant funds from the Department of Education in the amount of $15,000 on or about July 1, 2024. Through the investigation, it was determined that Jackson used an online payment platform to send a payment of $10,000 to a separate financial institution using a bank account that was in the name of Jackson and her husband.

Jackson made several withdrawals of grant funds over a period of three months while serving as Executive Director and completed approximately 180 deposits directly from AICA accounts for her own personal use.

The investigation also revealed Jackson purchased cashier's checks with AICA funds to make unauthorized purchases and used AICA funds to pay for unauthorized subscription streaming services. Jackson embezzled over $1.7 million of the grant funds. (Source)

Google Employee Charged With Obtaining $1.2 Million+ By Trading Confidential Business Information On Polymarket Betting Platform - May 27, 2026

Michelle Spagnuolo was a software engineer at Google. Spagnuolo had access to Google's internal data systems, including an internal software tool that provided him with access to confidential, nonpublic data.

Spagnuolo created an account on Polymarket, which is a prediction marketplace, in May 2024. That account was known as "AlphaRaccoon." Shortly after accessing Google's internal information, Spagnuolo used the AlphaRaccoon account to place trades in various markets on Polymarket.

In total, from on or about October 15, 2025, through on or about December 4, 2025, Spagnuolo used the AlphaRaccoon account to risk approximately $2,754,092 on markets related to Google's internal information.

Soon after Google's information was publicly announced, and the markets resolved, Spagnuolo's AlphaRaccoon account profited approximately $1.2 million based on his use of inside information in connection with bets placed on Polymarket. (Source)

Company Chief Financial Officer Pleads Guilty To Embezzling $739,000+ - June 4, 2026

Pamela Aguilar, 65, was employed as Chief Financial Officer of a software company in Connecticut.

Between approximately 2018 and 2025, Aguilar defrauded her company by making ACH and wire transfers from the company's bank account to personal bank accounts, writing checks and making cash withdrawals from company's bank account, and by making PayPal and credit card payments from the company's account for her own benefit.

Aguila stole more than $739,466.44 from her company A. She attempted to cover up her criminal behavior by providing false weekly cash reports and false monthly financial statements to company Chief Executive Officer. (Source)

Business Financial Controller Convicted Of Embezzling $598,000+ From Her Employer - May 28, 2026
Deborah Beaudoin, 56, was convicted of wire fraud for orchestrating a scheme that caused over $598,000 in losses to the business where she worked. Beaudoin admitted to devising and executing a scheme to order and obtain unauthorized company debit cards linked to the company's bank account.

Beaudoin made repeated false and fraudulent entries on company ledgers to make the withdrawal of money using these cards appear legitimate. Once Beaudoin obtained the cards, she withdrew the money at local ATMs and deposited a portion of those funds into her personal bank accounts. Over the five-year scheme, Beaudoin obtained at least $598,000 in fraudulent funds. (Source)

Employee At Financial Institution Sentenced To Prison For Stealing $168,000 - June 5, 2026
Between September 2021 and February 2022, Michael Torres, 38, was employed as a Relationship Manager at Financial Institution.

While in this position, he misused his position to apply for loans through financial institution in the names of individuals without their knowledge or authorization. Torres applied for 19 loans for a total of $168,000, which was deposited into bank accounts that he controlled. (Source)

Company Investment Analyst Charged With Insider Trading That Made Him $350,000+ June 5, 2026
Jianqing Li made more than $350,000 in illicit profits by trading in stock and options based on material, nonpublic information he misappropriated from the investment fund where he worked.

Li was an analyst at a Manhattan-based asset manager specializing in biomedical and healthcare investments, which routinely received nonpublic information from investment banks in connection with its evaluation of investment opportunities in public companies. Li repeatedly used inside information to trade securities for his own profit, in violation of his duties to his employer and to the sources of the information. (Source)

Boyfriend Who Misappropriated Confidential Documents From Girlfriend's Employer Charged For $2.7 Million Insider Trading Scheme - June 23, 2026
Between February 2022 and October 2024, Justin Jennings made well-timed trades in the securities of eight publicly traded companies in the days before major corporate announcements, based on material nonpublic information (MNPI).

At the time of these trades, Jennings was romantically involved with an account executive at a public relations firm that was entrusted with MNPI regarding these announcements.

Jennings' profitable bets came after he gained access to confidential information, including draft press releases, from his girlfriend's employer-issued laptop without her knowledge or permission. In total, Jennings made over $2.7 million in illegal trading profits from the scheme. (Source)

Engineering Manager Charged With Insider Trading Scheme That Made Him $1.4 Million+ - June 24, 2026
Casey Muggleston, 44, served as an engineering manager with a publicly traded energy company that operates nuclear, hydroelectric, wind, and solar generation facilities.

From in or around May 2024 until in or around September 2024, Muggleston learned of material nonpublic information about the company's efforts to restart a nuclear reactor.

The energy company owned the nuclear reactor, which had previously ceased operations in 2019. Muggleston received progress updates and confidential internal communications about the energy company's efforts to restart the reactor.

Muggleston used this confidential information to purchase hundreds of call options in the energy company through his own brokerage account. Muggleston purchased these call options despite his employer's policies prohibiting insider trading and the purchase and sale of the company's call options. On September 20, 2024, the energy company publicly announced the restart of the nuclear reactor and that it had entered into a power purchase agreement with a large technology company to purchase all of the energy produced by the reactor. That same day, Muggleston sold 550 call option contracts he held in the energy company for a total of approximately $1,480,380.67. (Source)

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

Director For Brooklyn New York Daycare Pleads Guilty Stealing $2.7 Million / Used Funds For Travel, Entertainment, Etc. - June 11, 2026

Murielle Misczak was hired by a daycare center in 2013 as Program Coordinator and was later promoted to Director in 2020.

Starting in January 2022 and continuing through October 2025, Misczak stole more than $2.75 million in tuition payments by directing them to be paid into accounts she controlled and then transferring those payments into her own accounts. Misczak hid her theft from the daycare center by deleting and altering information in the accounting systems. Misczak spent over $600,000 in stolen funds on travel and entertainment, including over $350,000 on tickets to professional wrestling events, as well as hundreds of thousands of dollars on luxury goods and various personal expenses such as food delivery and ride sharing services. (Source)

City Director For Department Of Elder Services Sentenced To Prison For Embezzling $136,000+ Of City Funds / Used Funds To Purchase 153 Pounds Of Steak, Toyota Prius, Etc. - June 17, 2026

Thomas Clasby was the Director of the Quincy Department of Elder Services in Massachusetts between approximately 1999 and April 2024.

Beginning in 2019, Clasby used the City's purchasing process to pay personal expenses and generate cash for himself. Clasby arranged for the City to pay $8,950 to a music studio to produce recordings of Clasby singing songs; $2,236 to food service vendors for 153 pounds of bourbon steak tips; $4,800 for a Toyota Prius; and $1,658 for a signature, lacquered, mounted and framed self-portrait, all of which were personal expenses.

In addition, Clasby arranged for the City to pay over $38,000 to a New York consulting company owned by Clasby's friend. The consulting company never provided goods or services to any city department. Instead, Clasby's friend cashed the city checks and delivered the cash to Clasby at a rest stop in Framingham, Mass., a ferry terminal in Bridgeport, Conn. and at the friend's New York apartment. Starting in June 2021, Clasby stole the majority of cash receipts generated by Elder Services at the Kennedy Center in Quincy. (Source)

Company Treasurer Sentenced To Prison For Embezzling $123,000 To Pay For Gambling Debts & Shopping - June 3, 2026

Katherine Henderson, 55, was employed as the treasurer for a manufacturer of brake products in Norfolk and had access to the company's financial records and accounts, including the ability to approve payroll.

To cover losses incurred through online gambling and to support her shopping habit, Henderson embezzled funds from the company by issuing herself unauthorized payroll funds above her salary. She also created a payroll account for her husband despite the fact he never worked for the company and was unaware that Henderson had created a payroll account for him.

Henderson intercepted vendor payments and diverted them to her personal accounts, then changed the company's records to make it appear the payments had been successfully deposited into company accounts. Henderson's fraud was discovered in August 2023 while she was on vacation. During her absence, a company employee requested payment from a vendor. The vendor provided proof that the payment had already been made and an investigation revealed that the payment had been diverted to Henderson's account. In total, Henderson embezzled $123,104.42 from her employer. (Source)

Company Chief Financial Officer Sentenced To Prison For Stealing $100,000+ / This Was Second Theft After Previously Serving Prison Time For Stealing $5 Million+ - June 8, 2026

Aaron Vallett, 48, was sentenced to 2 years and 2 months in federal prison, followed by a 3-year term of supervised release, and ordered to pay restitution in the amount of $101,630.56 for two counts of wire fraud.

Between July 2020 and November 2021, Vallett, as the Chief Financial Officer for a local home remodeling company, stole more than $100,000 from his employer. He used access to the company's bank account, granted to him by virtue of his position, to devise and execute a scheme to steal the company's funds for his own use and benefit.

Vallett was previously convicted in 2012 of mail fraud, wire fraud, and theft from an ERISA plan, for which he was sentenced to 10 years in federal prison, followed by three years of supervised release, and ordered to pay restitution in the amount of $5,492,548.77. Vallett's current scheme began almost immediately after his release from his 2012 conviction, while he was on supervised release. (Source)

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

School IT Department Employee Sentenced To Prison For Computer Sabotage After Termination / Download 300+ Usernames & Passwords Before Termination - June 17, 2026

Ezekiel Potter, 34, was terminated from his job in the IT department of Saydel Community School District in Iowa in April 2023. Prior to his termination, Potter downloaded over 300 usernames and passwords for school accounts and programs, which he used over the next year and a half to access or attempt to access various school online accounts and applications to disrupt the school district operations.

The attacks began in June 2023 when Potter took down one of the school's social media pages. After that, Potter began trying to revoke school employee access to critical systems and delete accounts and information. When successful, this resulted in districtwide technology outages and required significant remediation efforts from other district employees, among other interruptions. Potter's misconduct culminated in a series of attacks in January 2025 that resulted in suspending classes for multiple hours.

It was later determined Potter orchestrated many of the attacks from the offices of his subsequent employers. At one of those employers, Potter left a USB drive that contained hundreds of District usernames and passwords, along with other sensitive District information. After realizing he left the drive behind, Potter attempted to have a former coworker to "wipe" it.

In addition to his sentence of imprisonment, Potter was sentenced to three years of supervised release and ordered to pay $59,668.81 in restitution to the Saydel Community School District and its insurer. (Source)

THEFT OF ORGANIZATIONS ASSESTS / DESTRUCTION OF PROPERTY

Electrician Charged With Embezzling $200,000 From Employer By Stealing & Selling Wire To Scrap Yard - June 22, 2026

From October 2004 through February 2022, Clyde Hatton was employed in various electrician-related roles by his company, a corporation that designs, manufactures, and distributes engines and vehicle parts. As part of his employment, Hatton was issued an employee credit card for business-related expenses.

Beginning in October 2020, Hatton carried out a scheme to defraud his employer by purchasing wire and other equipment with no intention of using the items for work duties. Instead, he sold the wire to a scrap yard and kept the proceeds for his personal use. Hatton concealed the scheme by submitting receipts and falsely claiming the purchases were legitimate business expenses. In total, Hatton embezzled approximately $202,173.51 from his employer and sold fraudulently obtained wire to the scrap yard 107 times. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Virgin Islands Police Department Commissioner & OMB Director Both Sentenced To Prison For $100,000 Bribery Scheme For $1.4 Million Contract - June 12, 2026

Ray Martinez, is the former Commissioner of the Virgin Islands Police Department (VIPD), and Jenifer O'Neal, is the former Director of the Virgin Islands Office of Management and Budget (OMB).

Both were sentenced this week for their roles in a procurement fraud, bribery, and money laundering scheme. Martinez was sentenced to 10 years in prison and three years of supervised release, and O'Neal was sentenced to seven years in prison.

Martinez accepted nearly $100,000 in bribe payments from a government contractor, David Whitaker, who gave Martinez cash and payment for luxury travel, personal expenses, private-school tuition, and restaurant equipment.

In exchange for these payments, Martinez used his official authority to approve invoices submitted by Whitaker and also awarded Whitaker's company a $1.4 million dollar contract funded by the American Rescue Plan Act.

O'Neal, who served as the territory's chief budget official, knowingly approved a $70,000 inflated invoice under that same contract and later accepted a $17,730 lease payment for her business, Java Grande, using federal funds from the inflated invoice. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Hospital Nurse Sentenced To Prison For Stealing Controlled Substances For Her Own Use - June 11, 2026

Lauren Hornbuckle, 37, was a Florida-licensed registered nurse who worked at hospital.

Between November 2023 and March 2024, Hornbuckle tampered with injectable controlled substances, including morphine, hydromorphone, and fentanyl, by removing them from their containers and replacing them with saline. She then returned the containers into circulation for other patients' medical needs and used the drugs for her own personal use. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

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

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

Amazon Employee Charged With Murder Of Co-Worker - June 8, 2026

Police said Quentin Williams Jr., 20, faces a murder charge in a shooting that happened in the control-accessed parking garage of the Amazon Fulfillment Center in Illinois

An investigation determined the shooting stemmed from a domestic-related dispute between Williams and another Amazon employee, who was with the victim, Travion Taylor, 27, of Chicago, at the time. A physical altercation ensued and Williams pulled out a gun and fired multiple shots towards the two other employees, striking Taylor in the back. Williams then fled the scene. Taylor was transported to Loyola Hospital where he was pronounced dead. (Source)

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
www.insiderthreatincidents.com

INSIDER THREATS DEFINITION / TYPES

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

The information complied below was gathered from research conducted by the National Insider Threat Special Interest Group (NITSIG), and after reviewing NITSIG Monthly Insider Threat Incidents Reports.

WHO CAN BE AN INSIDER THREAT?

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

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

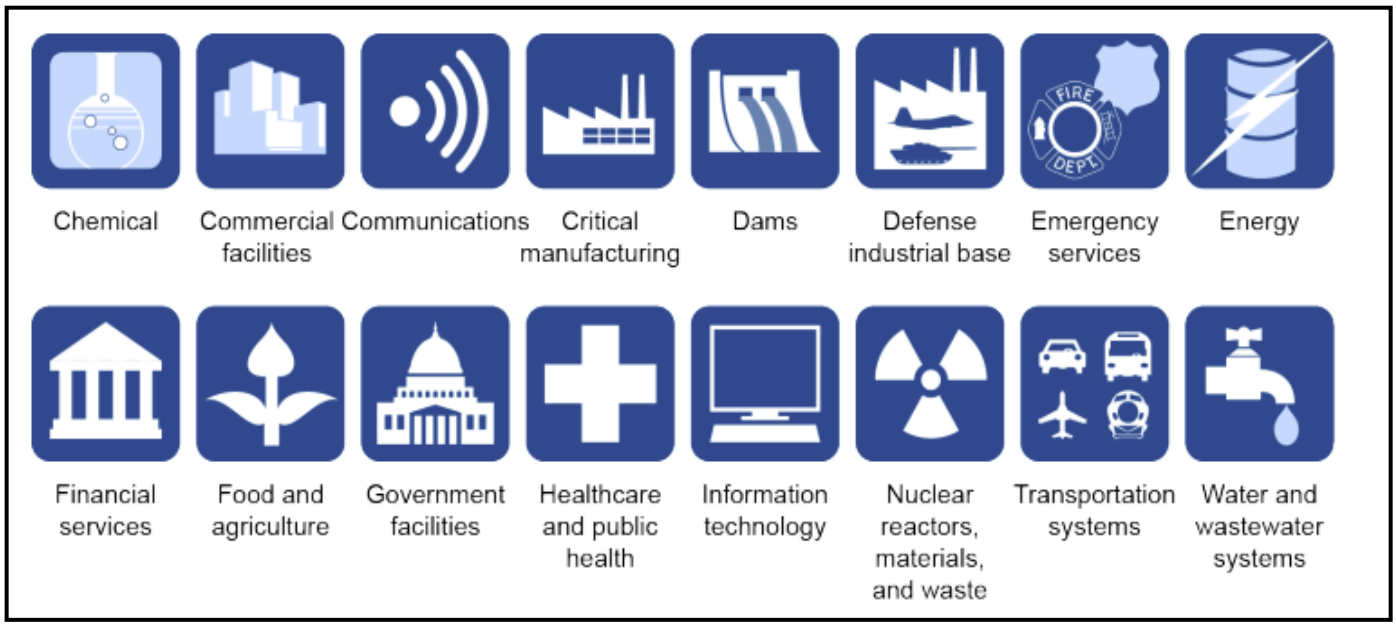
Other Damaging Impacts To An Employer From An Insider Threat Incident

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

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

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



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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

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

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

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

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

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

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

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

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

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

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

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

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

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

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

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

Fraud In Government Organization's / Infographic

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

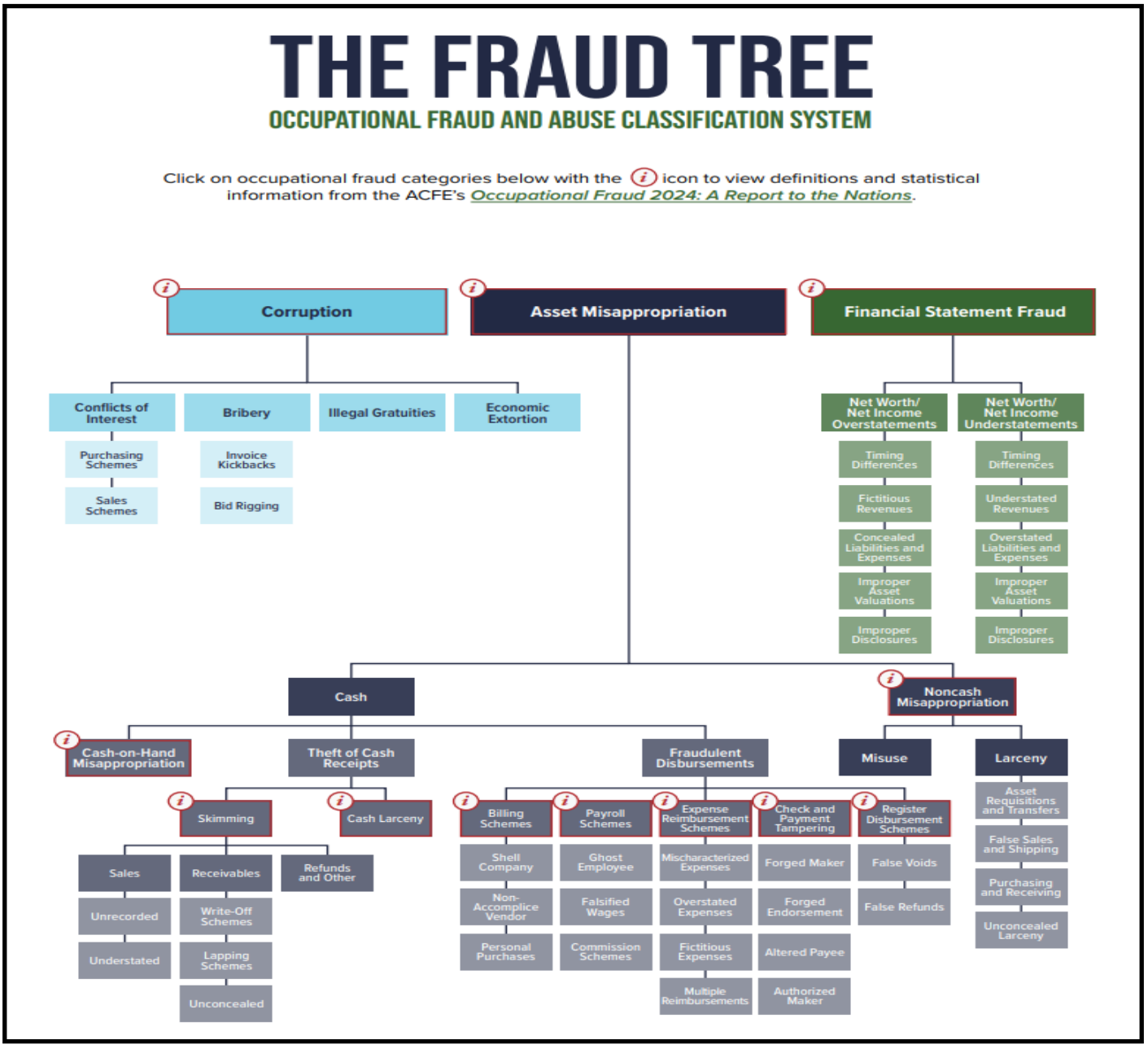
Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators



SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TRADE SECRET THEFT / DATA BREACHES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy.

Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lyons initiated the fraud shortly after he became CEO in 1999.

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

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

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

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

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

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

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

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

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

EMPLOYEE EXTORTION

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

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

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

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

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

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 (**7,200+ Incidents**).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

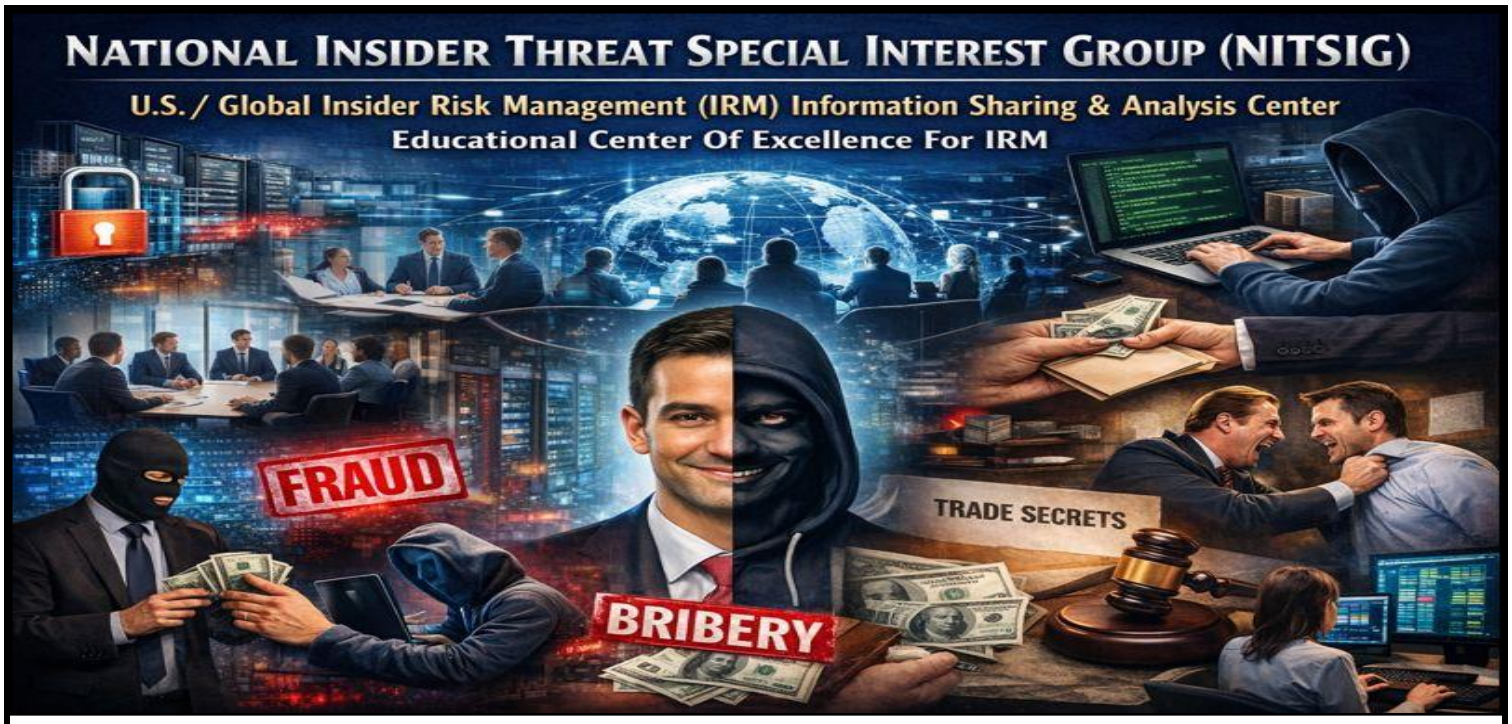
Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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

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

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

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



NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together Insider Risk Management (IRM) and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal **FREE OF CHARGE**.

NITSIG Membership

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

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

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

NITSIG Meetings

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

NITSIG Insider Threat Symposium & Expo (ITS&E)

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

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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with over 900 members enables the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

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

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

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

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

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

CONSULTING SERVICES OFFERED

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

BACKGROUND ON ITDG EXPERTISE IN THE FIELD OF INSIDER RISK MANAGEMENT

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

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

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

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

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

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

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

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

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

CLIENT SATISFACTION / COMPANY RECOGNITION

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

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

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

The ITDG Has Provided IRMP Training & Consulting Services To An Impressive List Of 700+ Clients:
White House, U.S. Capital Police, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. (Client Listing)

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

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

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