



INSIDER THREAT INCIDENTS REPORT
FOR
December 2024

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

TABLE OF CONTENTS

	<u>PAGE</u>
Insider Threat Incidents Report Overview	3
Insider Threat Incidents For December 2024	4
Definitions of Insider Threats	28
Types Of Organizations Impacted	28
Insider Threat Damages / Impacts Overview	29
Insider Threat Motivations Overview	30
What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations	31
2024 Association Of Certified Fraud Examiners Report On Fraud	32
Fraud Resources	33
Severe Impacts From Insider Threat Incidents	34
Insider Threat Incidents Involving Chinese Talent Plans	57
Sources For Insider Threat Incidents Postings	59
National Insider Threat Special Interest Group Overview	60
2025 Insider Threat Symposium & Expo	62
Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview	63

INSIDER THREAT INCIDENTS

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 **5,900+** 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 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 thousands of dollars 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 25** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS

FOR DECEMBER 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

U.S. Postal Service Employee Sentenced To Prison For Stealing 47 U.S. Treasury Checks Totaling \$750,000+ - December 27, 2024

Zerion Franklin was a United States Postal Service employee at the mail processing annex in Fayetteville, North Carolina.

In June 2024, the Fayetteville Police Department conducted a traffic stop of Franklin's vehicle. After observing drug paraphernalia in plain view, officers conducted a search of the vehicle. During the search, officers located 47 U.S. Treasury checks made payable to entities and individuals other than the defendant. The checks, which were dated between April and May of 2023, included federal tax refunds, VA benefits, and social security disability benefits. Officers also located marijuana packaged for sale, a loaded 9mm handgun, and over \$22,000 in U.S. currency.

Shortly after the traffic stop, an elderly victim in New Hanover County reported the theft of her tax refund check. It was later revealed that the check was stolen from the mail stream, altered to reflect Franklin's name as the payee, and cashed at a Walmart in Fayetteville on or about May 3, 2023. In total, investigators determined that Franklin stole U.S. Treasury checks totaling over \$750,000. ([Source](#))

U.S. Postal Service Employee Convicted Of Threatening To Shoot And Kill Employees Of The New York State Department Of Labor - December 13, 2024

Quadri Garnes was employed as a mail carrier for the United States Postal Service (USPS) at the Homecrest post office in Brooklyn, New York, from March 26, 2022 to May 29, 2022.

After crashing his postal truck into two vehicles, Garnes was terminated on May 31, 2022. Garnes subsequently applied for unemployment benefits but was denied because he had worked for the USPS for fewer than 60 days and was thus ineligible to receive benefits. On the morning of September 29, 2022, Garnes called the New York State Department of Labor (DOL) and was advised that he had worked for the USPS for too short a period to be eligible to receive benefits. In response, he threatened to shoot and kill employees of the USPS and DOL. During the 45-minute recorded call with two DOL employees,

Garnes's Statements Included:

- If I go back to the post office, I'm gonna shoot somebody.
- Y'all gonna make me go to jail for killing somebody.
- Do the city want me to kill five or six different people?
- I got 18 and a half years in jail. It don't bother me to be in jail. I made myself, meaning like I'm made, as long as I'm in the New York City jail, I'm good.
- You might see this s--t on TV. Just remember my name. You might see it on TV tonight. You, just remember my name!
- Somebody might get shot today coming out of Department of Labor.
- Believe me, I'll be at the New York State Department of Labor down on Schermerhorn or Livingston Street and I will make a big f---ng deal out of it.

Garnes's threats triggered an immediate response by the DOL, the New York State Police and by Postal Inspectors, who took precautions against Garnes's return to the postal facility where he had briefly worked and the DOL office he named. Garnes was arrested approximately two weeks after making his threats. ([Source](#))

U.S. Postal Service Office Manager Charged With [Stealing \\$81,000+ Of Stamps](#) - December 21, 2024

Emilio Chirico, the Station Manager for the DeWitt, New York Post Office, has been charged by indictment with wire fraud, misappropriation of postal funds, and false entries and reports

Between January 2021 and March 2023, Chirico stole \$81,553.94 in stamps from the DeWitt Post Office and falsified postal records to conceal the theft of the stamps. Chirico has been the station manager at the DeWitt Post Office since March 2012. ([Source](#))

U.S. Postal Service Employee Sentenced To Prison For [Stealing \\$3,300 In Money Orders](#) - December 11, 2024

Between on or about December 1, 2023, and April 16, 2024, Tiffany Isenhardt stole \$3,380 in money orders while employed at the Charmco Post Office in West Virginia, and converted them to her own use. Isenhardt admitted that she used her position as a United States Postal Service employee to issue the money orders to herself without paying for them or paying the associated fees. ([Source](#))

Former U.S. Postal Service Employee Guilty Of Delaying And Stealing Contents Of U.S. Mail - December 13, 2024

Between on or about July of 2022, through October 4, 2022, Randy Brown unlawfully secreted, detained, and delayed U.S. mail, entrusted to him as a postal employee; and on September 26, 2022, September 27, 2022, and October 3, 2022, Brown did knowingly embezzle, steal, abstract, and remove checks from U.S. mail, entrusted to him as a postal employee. ([Source](#))

U.S. Postal Service Supervisor Accused Of [Stealing 90 Checks From Mail](#) - December 26, 2024

On Oct. 31, 2023, Benita Randle stole about 90 checks from mail that had been entrusted to the Postal Service for delivery.

Randle was a supervisor at the St. Louis Processing and Distribution Center in St. Louis at the time. ([Source](#))

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Army National Guard Soldier Charged With Murder - December 16, 2024

Natravien Landry is an Army National Guard soldier assigned to the 1148th Transportation Company at Fort Eisenhower.

He is alleged to have visited the residence in post housing at Fort Eisenhower early Saturday morning, Dec. 14, of a woman with whom Landry shares a child. Landry is accused of assaulting and shooting a man who was with the woman in her residence, and then leaving Fort Eisenhower. Landry was arrested about three hours later south of Atlanta on Interstate 85 during a traffic stop by the Meriwether County, Georgia, Sheriff's Office, and deputies recovered a 9 mm pistol during the stop. ([Source](#))

CIA Official Charged For Leaking Classified Information About Israel's Plans To Strike Iran - November 13, 2024

A CIA official has been charged with leaking highly classified US intelligence about Israel's potential plan to retaliate against Iran for a missile strike earlier this year.

Asif W. Rahman, who worked overseas for the agency and held a top-secret security clearance, was arrested by the FBI in Cambodia and indicted under the Espionage Act.

The files, which were prepared by the National Geospatial-Intelligence Agency, in part detailed satellite imagery tied to the potential Israeli strike, as well as the various kinds of missiles on hand. They were posted by a telegram account called "Middle East Spectator." ([Source](#))

Office Manager Sentenced To Prison For [\\$1.3 Million](#) Fake Invoice Fraud Scheme For U.S. Marine Forces Reserve - July 31, 2024

Kamila Dudley employed by Company A from September 2008 through March 2023; and, from March 2017 through November 2018. Dudley served as Company A's Office Manager. As Company A's Office Manager, Dudley prepared and submitted Company A's invoices for payment.

In approximately March 2017, Company A subcontracted with Company B to provide onsite support services at the Marine Forces Reserve (MARFORRES) facility in New Orleans, Louisiana. Company A, by and through multiple employees, committed wire fraud by knowingly submitting materially false invoices to Company B, knowing that Company B would, in turn, present the false information to the United States for payment.

From March 2017 through November 2018, Company A billed the United States, through Company B, for services not provided. The fraudulent invoices included the names of Company A's executives, who performed no work at MARFORRES. The fraudulent invoices also included the names of certain individuals who worked full-time on a separate contract at a separate facility and, thus, performed no work at MARFORRES. Because neither Company B nor the United States was aware of the fraudulent nature of the invoices, Company A was paid approximately \$1,300,000 under the subcontract. ([Source](#))

3 Active Duty U.S. Army Soldiers Convicted For Fraudulently [Obtaining \\$100,000+ In COVID-19 Related Loans](#) - December 3, 2024

Major Eduwell Jenkins, Sergeant First Class Crispin Abad and Sergeant Malaysia Stubbs filed for fraudulent PPP loans in 2021.

Though they were active-duty soldiers, Jenkins and Stubbs falsely represented to the Small Business Administration (SBA) that they each had jobs separate from their military employment that generated over

\$100,000 in annual income. To substantiate this false income, Jenkins and Stubbs generated fabricated Internal Revenue Service (IRS) tax return forms, submitting them to the SBA as supporting documentation for the PPP applications. Jenkins and Stubbs never submitted these falsified tax return forms to the IRS as part of legitimate tax filings. Based on their false submittals, Jenkins and Stubbs each received over \$20,000 in government-backed PPP loans to which they were not entitled.

Abad allegedly received over \$41,000 in PPP loans to which he was not entitled.

Abad then allegedly used fraudulently obtained funds for various luxury and recreational spending, including purchases at the Fort Gregg-Adams Golf Course, Ace Adventure Resort in West Virginia, Victoria's Secret, Sunglass Hut, and the Virginia ABC Store. Additionally, Abad allegedly purchased jewelry at Reeds Jeweler and withdrew hundreds of dollars in fraud proceeds at the MGM Casino in National Harbor, Maryland. ([Source](#))

3 individuals Plead Guilty In Conspiracy Scheme Involving The Bribery Of A U.S. Army Government Contracting Officer - December 19, 2024

Francisco Guerra, Coogan Preston and Jason Ingram pleaded guilty to conspiracy to bribe a public official. Preston also pleaded guilty to receiving a gratuity as a public official.

According to the plea agreements, the scheme began in 2016 and continued until 2021. As part of the scheme, Guerra agreed to provide money and other items of value to Preston, a government contracting official working at Redstone Arsenal in Huntsville, Alabama. In exchange for these bribes, Preston identified subcontracting opportunities for companies owned and operated by Guerra and convinced the prime contractor to use one of Guerra's companies as a subcontractor. ([Source](#))

3 U.S. Army Soldiers Arrested On Human Smuggling Conspiracy Charges - December 4, 2024

3 Fort Cavazos soldiers were arrested on criminal charges related to their alleged involvement in a conspiracy to smuggle undocumented noncitizens.

The U.S. Border Patrol Agent initiated a vehicle stop in Presidio on Nov. 27. The vehicle fled as the agent approached the passenger side and struck a second USBP vehicle, injuring an agent inside, according to the filed criminal complaint. Presidio County Deputies and Presidio Police Officers eventually stopped the vehicle and apprehended four individuals, three of whom were undocumented noncitizens—one Mexican national and two Guatemalan nationals.

The fourth individual was Emilio Mendoza Lopez, who claimed to be the front seat passenger in the vehicle. The driver, alleged to be Angel Palma, fled on foot and was located the following day at a hotel in Odessa.

Mendoza Lopez and Palma allegedly traveled from Fort Cavazos to Presidio for the purpose of picking up and transporting undocumented noncitizens. A third individual, Enrique Jauregui, is alleged to be the recruiter and facilitator of the human smuggling conspiracy. Data extracted from Palma's phone through a search warrant revealed messages between the three soldiers indicating collaboration in the smuggling operation. ([Source](#))

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Law Enforcement Officer Sentenced To Prison For **\$2.4 Million+ COVID-19 Pandemic Relief Program Fraud Scheme - December 6, 2024**

Richard Hebert was sentenced to prison following his conviction for making a false statement to a bank in connection with numerous fraudulent applications that he filed to obtain funds from the Paycheck Protection Program (PPP).

Between April of 2020 and July of 2020, Hebert submitted at least 12 fraudulent PPP loan applications on behalf of seven different companies to five different banks seeking more than \$4.2 million in PPP loan funds,

that were designed to provide emergency financial assistance to the millions of Americans who were suffering from the economic effects caused by the COVID-19 pandemic.

On these applications, Hebert made false representations regarding his businesses and their operations.

In support of these fraudulent applications, Hebert created false tax forms and other documents, which included the real personal identifiable information of people to facilitate his crime. Hebert's pandemic fraud scheme caused a loss of more than \$2.4 million.

Hebert was ordered to pay \$2,450,639.93 in restitution to the United States Small Business Administration.

Previously in the investigation, the United States seized a significant share of the proceeds from the offense, as well as a residence in New Orleans, and three vehicles, including a 2013 Ghost Rolls Royce, a Lexus ES 350, and Ford F-250. ([Source](#))

Virginia Sheriff Convicted In \$75,00 Bribery Scheme - December 19, 2024

A former sheriff of Culpeper County, Virginia, was convicted by a jury in Charlottesville, Virginia, yesterday for accepting over \$75,000 in bribes in exchange for appointments as auxiliary deputy sheriffs.

Scott Jenkins accepted cash bribes and bribes in the form of campaign contributions from co-defendants Rick Rahim, Fredric Gumbinner, and James Metcalf, as well as at least five others, including two FBI undercover agents. In return, Jenkins appointed each of the bribe payors as auxiliary deputy sheriffs, a sworn law-enforcement position, and issued them official Culpeper County Sheriff's Office badges and credentials. The bribe payors were not trained or vetted and did not render any legitimate services to the Sheriff's Office. In addition, Jenkins pressured other local officials to approve a petition filed in Culpeper County Circuit Court by Rahim, a convicted felon, to restore his right to possess a firearm and which falsely stated that Rahim resided in Culpeper County. ([Source](#))

Correctional Officer Sentenced To Prison For Accepting \$45,000+ In Bribes From Inmates To Smuggle Cell Phones Into Facility - December 5, 2024

Stephen Crittenden was a California Department of Corrections and Rehabilitation correctional officer at the California Medical Facility in Vacaville.

From 2021 through 2023, he accepted bribes from inmates, totaling more than \$45,000, to smuggle cellphones into the California Medical Facility. ([Source](#))

Miami Correctional Officers Charged With Running A Criminal Enterprises - December 20, 2024

Vernell Lawson, a former Miami-Dade Correctional Officer, and Gabrielle Bess-Mills, made their initial appearance in court on a previously sealed indictment containing charges related to a continuing criminal enterprise led by co-defendant Terrance Carter

Carter led a drug trafficking organization which relied on the corruption of Lawson and other Miami-Dade Correctional Officers, along with drug trafficking associates, to introduce narcotics and other contraband for sale into Miami-Dade County jail facilities. ([Source](#))

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Director Of Public Library Sentenced To Prison For [Embezzling \\$770,000+ / Used Funds For Mortgage Payments, Auto Repairs, Etc.](#) - December 19, 2024

From 2009 to 2019, Xavier Menzies misappropriated approximately \$770,715 from the library. Much of the money was initially received by the Markham library from the public library district in nearby Posen, Ill., which paid Markham for allowing Posen residents to access the library and use its services.

Menzies opened bank accounts in the name of Markham Public Library and deposited checks made out to the library. He later withdrew the funds and used the money for personal expenses, including mortgage payments, ticket purchases, and auto repairs. Menzies concealed the scheme by routinely misrepresenting the library's financial condition to the Markham Public Library's Board of Trustees.

As part of the fraud scheme, Menzies also increased his annual salary as library director without the approval or knowledge of the Board of Trustees and continued to receive the higher salary for approximately three years. ([Source](#))

New York City Housing Authority Superintendent Convicted Of Bribery & Extortion For Accepting Cash From Contractor In Exchange For Awarding Contracts - December 13, 2024

New York City Housing Authority (NYCHA) is the largest public housing authority in the country, providing housing to New Yorkers across the City and receiving over \$1.5 billion in federal funding from the U.S. Department of Housing and Urban Development (HUD) every year.

When repairs or construction work at NYCHA housing require the use of outside contractors, services must typically be purchased via a bidding process. However, when the value of a contract was under a certain threshold, designated staff at NYCHA developments, including superintendents, could hire a contractor of their choosing without soliciting multiple bids. With either type of contract, a NYCHA employee needed to certify that the work was satisfactorily completed in order for the contractor to receive payment from NYCHA.

Gilmore, a superintendent at three NYCHA developments in the Bronx between 2016 and 2023—Bronx River Houses, Eastchester Gardens, and Forest Houses—demanded and received cash in exchange for NYCHA contracts. GILMORE typically demanded \$1,000 for each contract he awarded.

In total, GILMORE demanded and received tens of thousands of dollars in bribes in exchange for hundreds of thousands of dollars in NYCHA contracts.

[Of the 70 individual NYCHA employees charged with bribery and extortion offenses in February 2024, 59 have pled guilty, and three have been convicted after trial.](#) ([Source](#))

2 California City Officials Plead Guilty Accepting Bribes In Exchange For Politician's Votes And Influence Over City's Permitting Process - December 5, 2024

Edgar Cisneros served as Commerce's City Manager from November 2017 to December 2023. Robert Tafoya served as a city attorney from December 2013 to October 2022.

Shortly after Baldwin Park began issuing marijuana permits in June 2017, Baldwin Park City Councilmember Ricardo Pacheco solicited bribes from companies seeking those permits.

Cisneros helped a company obtain a marijuana permit and related approvals through approximately \$45,000 in bribes and that the company promised to pay Cisneros at least \$235,000 to help secure the permit.

Tafoya facilitated a bribery scheme involving former Compton City Councilmember Isaac Galvan, in which Galvan sought to obtain a marijuana permit for his consulting client also through bribes to Pacheco. ([Source](#))

SCHOOL SYSTEMS / UNIVERSITIES

Former School Maintenance Director Charged For Scheme To Defraud County Schools Out of \$3.4 Million - December 11, 2024

Michael Barker was the Maintenance Director from in or about 2015 through in or about November 2023, and was responsible for ordering supplies necessary for the maintenance of the Boone County schools.

Barker falsified documents showing that the Boone County Board of Education was receiving large amounts of janitorial and custodial products including hand soap, trash can liners, and face masks from Rush Enterprises, a

Kentucky business with an office in Kenova, West Virginia, when the Boone County Board of Education was only receiving a small amount of those products.

Acting in his capacity as maintenance director, Barker submitted fraudulent invoices and purchase orders that caused the Boone County Board of Education to pay for more than \$4,000,000 of products from Rush Enterprises. During calendar years 2022 and 2023, for example, Barker submitted invoices to the Boone County Board of Education that caused them to pay Rush Enterprises for 4,993 cases of hand soap when, in fact, the Boone County Board of Education had only received approximately 829 cases. The Boone County Board of Education paid approximately \$474,696 for hand soap that was never delivered.

Barker defrauded the Boone County Board of Education out of approximately \$3,400,000. ([Source](#))

Assistant Graduate School Dean Sentenced To Prison For Role In Embezzling \$1.3 Million+ From Graduate School - December 6, 2024

The scheme involved Teresina DeAlmeida and her co-conspirators, Rose Martins and Silvia Cardoso.

Between 2009 and July 2022, DeAlmeida, Martins, and Cardoso conspired to fraudulently misappropriate more than \$1.3 million from their former employer, a graduate school of a university in Essex County, New Jersey.

During the scheme, DeAlmeida was an assistant dean responsible for financial functions, and Martins served as her assistant. Cardoso, DeAlmeida's sister, was also employed by the graduate school in a support staff role.

Beginning in 2009, DeAlmeida directed a graduate school vendor to pay Martins and Cardoso as though they worked for the vendor, even though they did not perform any services. DeAlmeida and Martins then caused the vendor to submit false invoices to the graduate school over the course of approximately four years to reimburse the vendor for the amounts fraudulently paid to Martins and Cardoso.

From 2010 through 2022, DeAlmeida and Martins directed graduate school vendors to order hundreds of thousands of dollars of gift cards and prepaid debit cards the co-conspirators used for their personal benefit, and then to submit fraudulent invoices to the school purporting to be for goods and services that were never provided. The co-conspirators also misused DeAlmeida's school-issued credit card to purchase hundreds of thousands of dollars of gift cards and prepaid debit cards from the school's bookstore.

DeAlmeida routinely fraudulently approved these charges and Martins forged the signatures of other employees on internal approvals.

In 2015, Martins opened a shell entity called CMS Content Management Specialist LLC. Although CMS never rendered any services to the graduate school, Martins submitted, and DeAlmeida approved, fraudulent invoices totaling more than \$208,000.

The co-conspirators also used DeAlmeida's school-issued credit card to make tens of thousands of dollars in unauthorized personal purchases.

For example, DeAlmeida and Martins used the card to make over \$70,000 in purchases at an online retailer shipped directly to their homes, including woman's shoes, smart watches, and bed linens. DeAlmeida and Martins fraudulently altered certain receipts before submitting them to the school for payment. ([Source](#))

School Treasurer Sentenced To Prison For [Theft Of \\$500,000+](#) - December 12, 2024

According to investigators, from June 2019 until October 26, 2021, while Treasurer of Hulbert Public Schools in Oklahoma, Leslie Mack issued herself and another individual excessive payroll payments above and beyond their district-authorized salaries. Mack also allowed another individual access to the financial accounting system. Their combined actions resulted in an ultimate loss to the Hulbert Public School District exceeding half a million dollars.

The Court ordered Mack to pay \$372,808.09 in restitution. ([Source](#))

Former Public Schools Payroll Services Director Pleads Guilty to Defrauding School District Of [\\$471,000+](#) - December 13, 2024

Between 2014 and April 2022, Kim Weinrich was employed by Mustang Public Schools (District) as Payroll Supervisor and was later promoted to Director of Payroll Services in 2021.

In her roles with the District, Weinrich was responsible for administering, processing, and reconciling the bi-monthly payroll for the District's employees.

Beginning in July 2016, Weinrich manipulated the District's payroll accounting software to increase her net pay each pay period, and deposited the stolen funds into her personal bank account. Weinrich's scheme resulted in several District employees underreporting their federal and state withholdings, which reduced the amount of their tax refunds. In all, between July 2016 and April 2022, Weinrich defrauded the District out of approximately \$471,657.91. ([Source](#))

High School Dean Charged For Role With Cocaine Trafficking Conspiracy - December 11, 2024

Lavante Wiggins, the Dean of Students at Pittsfield High School, operated a drug trafficking organization (DTO) that distributed large amounts of cocaine in and around the Pittsfield area.

It is alleged that Warren is a trusted member of the DTO who serves as a runner for Wiggins. According to the charging documents, in August 2024, Wiggins expressed concern that he was under investigation and that he would send Warren to complete drug sales and deliver cocaine. It is alleged that one of Wiggins' customers amassed a debt of more than \$34,000 for cocaine that Wiggins provided on credit. It is further alleged that Wiggins and Warren then went about collecting on that debt while continuing to supply large amounts of cocaine to that customer. Specifically, Wiggins allegedly directed

Warren to distribute cocaine to that customer on four separate occasions between September and December 2024: approximately 91 grams of cocaine on Sept. 10, 2024; approximately 100 grams of cocaine on Oct. 14, 2024; 125 grams of cocaine on Oct. 31, 2024; and 150 grams of cocaine on Dec. 10, 2024. ([Source](#))

CHURCHES / RELIGIOUS INSTITUTIONS

Priest Sentenced To Prison For [Stealing \\$300,000](#) In Church Funds - December 18, 2024

Ignazio Medina, a Catholic priest, was pastor at St. Stanislaus Catholic Church in Wardsville from 2013 to 2021.

Some financial irregularities arose at St. Stanislaus in 2018, and in the course of investigating the diocese discovered the parish had a bank account that was not previously reported on the budget or annual report. Medina was asked to include this bank account in the parish's annual report, and in 2020 he reported an account balance of about \$358,000.

After Medina was transferred to a different parish in 2021, it was discovered that he had emptied that bank account. While some expenditures from the account appeared to be church-related, on June 10, 2021, Medina had written a \$100,000 check to his sibling in Tucson, Arizona. The next day, he had also written a \$200,000 check payable to himself.

Medina, when confronted, claimed the bank account was funded by donations that were not intended for the parish itself, but rather were intended for his own discretionary use. Donors who had contributed checks deposited into the bank account contradicted Medina's statement.

Several individuals told investigators the checks they wrote to St. Stanislaus were intended for parish purposes, and that they never had any conversations with Medina authorizing a different use of the funds. One donor told investigators he intended his donation to be used in the school in memory of a deceased friend.

Medina also claimed he was refunding donations and that his sibling in Tucson was one of the donors. In fact, his sibling was not a source of donations to the account, and told investigators that Medina had said that the money was intended to care for their ailing mother. ([Source](#))

LABOR UNIONS

Union President Pleads Guilty To [Embezzling \\$36,000](#) - December 10, 2024

Between approximately August 2019 and December 2020, Leticia Russi-Shareno served as president of Local 2076 of the American Federation of Government Employees. Local 2076 is a labor union whose members are employees of the U.S. Department of Homeland Security working in Vermont and upstate New York.

As president, Russi-Shareno had check signing authority on Local 2076's Vermont bank account and also received a debit card to make official purchases on behalf of the union.

During her presidency, Russi-Shareno embezzled approximately \$36,000 from Local 2076's coffers by using the union's debit card to make ATM withdrawals of funds for personal expenses; using the debit card to make purchases for her personal benefit; and by falsifying paperwork to obtain duplicate reimbursements for expenses incurred on behalf of Local 2076. The defendant also cashed or deposited into her own account several checks that the national AFGE union had issued to Local 2076. ([Source](#))

BANKING / FINANCIAL INSTITUTIONS

TD Bank Employee Arrested And Charged With Facilitating Money Laundering For Bribes / [TD Bank Fined \\$1.8 BILLION](#) - December 11, 2024

Leonardo Ayala worked at a TD Bank store in Doral, Florida, between February and November 2023.

Starting in June 2023, Ayala exploited his position as a bank employee to facilitate money laundering. After another TD Bank employee opened accounts in the names of shell companies with nominee owners, Ayala assisted the money laundering network by issuing dozens of debit cards for the accounts in exchange for bribes.

Those accounts were then used to launder narcotics proceeds through cash withdrawals at ATMs in Colombia. The investigation has revealed that millions of dollars were laundered to Colombia through accounts Ayala serviced.

TD Bank pleaded guilty and agreed to pay over \$1.8 BILLION in penalties to resolve the Justice Department's investigation into violations of the Bank Secrecy Act and money laundering. ([Source](#))

Bank Attorney Pleads Guilty To [Embezzling \\$7.4 Million For 10 Years](#) - December 20, 2024

From approximately 2013 to January 2022, James Blose was an attorney and held high-ranking positions, including General Counsel, at Hudson Valley Bank and Sterling National Bank. From approximately January 2022, when Webster Bank acquired Sterling National Bank, until February 2023, Blose served as Executive Vice President and General Counsel and Corporate Secretary at Webster Bank.

From approximately 2013 until Webster Bank discovered his scheme and his employment was terminated in February 2023, Blose defrauded his employers (The Bank) in various ways.

In certain commercial loan transactions where The Bank was the lender, Blose fraudulently retained for himself portions of closing costs, including legal fees. In certain real estate transactions in which The Bank was the seller, Blose retained portions of the sale proceeds for himself. For some of the real estate transactions, Blose created false documents in order to hide his theft from The Bank. Blose also stole from The Bank in other ways.

As part of the scheme, used his attorney trust accounts to make personal expenditures, and to transfer funds to accounts in the names of business entities he created and controlled, and then used those funds for his personal benefit. Through this scheme, Blose stole approximately \$7.4 million from his employers. ([Source](#))

Bank Senior Vice President Sentenced To Prison For [Stealing \\$1 Million To Support His Gambling Debit](#) - December 13, 2024

Between February 2013 and December 2019, John Padilla served as senior vice president and commercial loan officer for a federally insured bank located in Lawton, Oklahoma.

During that time, Padilla executed a scheme in which he recruited borrowers to apply for loans, many of which were not creditworthy and were in fact Padilla's friends and associates.

Padilla told the borrowers he would use the loan proceeds to invest in his real estate ventures, and that he would pay the borrowers a percentage of the profit.

In reality, Padilla would use most of the loan proceeds to support his gambling habit, while also using proceeds to make payments toward prior loans issued as part of the scheme. In all, Padilla's actions cost the bank more than \$1,000,000. ([Source](#))

TD Bank Teller Arrested For [Stealing \\$180,000+](#) From Customer Accounts - December 19, 2024

BOSTON – A Saugus man has been arrested and charged for allegedly embezzling bank funds while working as a teller at TD Bank.

Derek Aut , 28, has been charged by criminal complaint with embezzlement by a bank employee. Aut was arrested yesterday and released on conditions following an initial appearance in federal court in Boston.

Derek Aut allegedly stole from the bank accounts of two TD Bank customers.

When one of the victims noticed money missing from her account, Aut allegedly attempted to cover up his theft by taking money from the other victim's account and depositing it into the first victim's account. In total, Aut is alleged to have taken more than \$180,000 from the victims' accounts. ([Source](#))

Citi Group Wins Court Order Against Former Employee Who Took Confidential Information Related To Citi Group's Law Firm Clients - November 27, 2024

A federal judge in San Francisco has temporarily blocked a former Citigroup banker from using confidential information related to Citi's law firm clients following his move to competitor Bank of Montreal (BMO).

The judge ordered John Mitchell, a former managing director in Citi Global Wealth at Work's law firm unit, to return any of the bank's records within 24 hours.

Citi showed that Mitchell "likely misappropriated its trade secrets in the form of confidential client information" and "likely breached" some of his contractual obligations to Citi.

Citi Bank and Citi Group Global Markets sued Mitchell and former Global Wealth at Work law firm unit senior vice president Benjamin Carr last week. The San Francisco-based bankers were among 18 from Citi who joined BMO's law firm wealth management group in a move announced last month. ([Source](#))

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Empower Pharmacy Accuses 4 Former Executives Of Conspiring To Steal Company Secrets To Setup Competing Company - December 21, 2024

Empower Pharmacy (The Company), one of the nation's leading compound pharmacies and outsourcing facilities, which services patients and clinics across the country, has accused several former executives, and others, of taking part in a conspiracy to brazenly steal valuable trade secrets the group used to set up a competing entity.

The conspiracy took shape among the executives and outside consultants as Empower undertook expansion plans in 2023 to meet the demand for its products, the Company claims in a Second Amended Complaint, filed in Federal Court in Houston, Texas.

To raise investor cash to fund the expansion, which included new production facilities, Empower produced investor decks highlighting its new business opportunities, financial projections, expense reports, and strategic plans. The former executives, then employed by Empower in key legal and financial positions, copied those documents, the lawsuit alleged.

The masterminds of the alleged conspiracy then set up a new entity whose aim would be to directly compete with Empower, according to the lawsuit.

The 4 former Empower employees downloaded and shared trade secrets among each other and their alleged co-conspirators, at times during regularly scheduled Friday morning video calls, it is alleged, before wiping the documents from their company computers. Others involved in the plot wiped their emails from their computers in an attempt to conceal their theft and improper plans, it is alleged.

As the conspiracy advanced and was still unknown to Empower, one by one the executives involved in the scam resigned their positions at the compound pharmacy. It was only after the executives had resigned and Empower undertook an analysis of their computers that the theft and conspiracy were uncovered, court papers reveal. ([Source](#))

2 Employees Being Investigated For Stealing Confidential Company Data And Sharing It With Competitor - December 5, 2024

"he police have registered an FIR against two former employees of Baccarose Perfume and Beauty Products Private Limited in Worli, a leading distributor of perfumes and beauty products, for allegedly stealing confidential company data and sharing it with a competitor.

The complaint was lodged by Laxman Patil, executive director of Baccarose, who alleged that the accused, identified as Vishwajeet Kakade, a former senior executive in the e-commerce department, and Sankesh Jaitapkar, a senior manager for brands, violated their employment agreements by emailing sensitive data to their private accounts before leaving the company.

Kakade joined the company in April 2021 and resigned in July 2024. Jaitapkar was employed from 2021 and left in July 2023 to join a rival firm. Both had signed agreements prohibiting activities that could harm the company's interests or lead to data breaches.

Kakade sent emails containing critical business information, including product sales data, pricing strategies, and demand forecasts, to Jaitapkar, who had already joined a competitor by then.

This information, considered vital for strategic planning and maintaining market position, is said to have been misused to benefit the rival company. ([Source](#))

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

University Of Delaware Pays \$715,000 Penalty For Not Disclosing Professor's Ties To People's Republic Of China - December 16, 2024

The University of Delaware (UD), located in Newark, Delaware, has agreed to pay \$715,580 to resolve civil allegations that it failed to disclose a UD professor's affiliations with and support from the government of the People's Republic of China in connection with federal research funding.

This settlement relates to a National Aeronautics and Space Administration (NASA) grant that was issued to UD in June 2020. Since 2011, federal law has prohibited NASA from using funds to collaborate with China or any Chinese-owned companies.

The settlement resolves allegations that UD caused NASA to violate this law by failing to disclose that one of the principal investigators on the grant was affiliated with the Chinese government through: (1) employment at a Chinese university; (2) participation in a program established by the Chinese government to recruit individuals with knowledge or access to foreign technology intellectual property; and (3) a grant from the National Natural Science Foundation of China. ([Source](#))

Employee / Resident Of China Sentenced To Prison For Stealing Trade Secrets From Of U.S. Electric Vehicle Company For His Own Business / [Made \\$1.3 Million+](#) - December 16, 2024

Klaus Pflugbeil was sentenced to prison for conspiring to send trade secrets that belong to a leading U.S.-based electric vehicle company (Victim Company-1).

Pflugbeil, a resident of the People's Republic of China (PRC) and a Canadian and German national, and his co-defendant, Yilong Shao, who remains at large, are owners of a PRC-based business (Business-1) that sold technology used to make batteries, including batteries used in electric vehicles.

Pflugbeil and Shao, former employees of a company that was purchased by Victim Company-1, took trade secrets from their employer, and later used the trade secrets to build a business that they marketed as a replacement for Victim Company-1's products. ([Source](#))

14 North Korean Nationals Charged For Concealing Their Identities To Pose As U.S. Information Technology Workers - December 12, 2024

A federal court indicted 14 nationals of the Democratic People's Republic of North Korea (DPRK or North Korea) with long-running conspiracies to violate U.S. sanctions and to commit wire fraud, money laundering, and identity theft.

The conspirators, who worked for DPRK-controlled companies Yanbian Silverstar and Volasys Silverstar, located in the People's Republic of China (PRC) and the Russian Federation (Russia), respectively, conspired to use false, stolen, and borrowed identities of U.S. and other persons to conceal their North Korean identities and

foreign locations and obtain employment as remote information technology (IT) workers for U.S. companies and nonprofit organizations.

The conspirators, some of whom were ordered by their superiors to earn at least \$10,000 per month, generated at least \$88 million throughout the approximately six-year conspiracy. In multiple instances, the conspirators supplemented their employment earnings by stealing sensitive company information, such as proprietary source code, and then threatening to leak such information unless the employer made an extortion payment.

Ultimately, the conspirators used the U.S. and PRC financial systems to remit the proceeds of their activity to accounts in the PRC for the ultimate benefit of the DPRK government. ([Source](#))

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

Doctor For Medical Company Agrees To Plead Guilty To Conspiring With Attorney To Defraud \$3 Million+ From California's Workers' Compensation Fund - December 16, 2024

A physician who worked for an Inland Empire medical company has agreed to plead guilty to conspiring to defraud California's workers' compensation fund of millions of dollars by continuing to work on workers' compensation matters after being suspended due to a prior health care fraud conviction,

Dr. Kevin Tien Do plead guilty that from October 2018 to February 2023, he conspired to defraud the state of California of millions of dollars of health care funds by defrauding California's Subsequent Injuries Benefits Trust Fund (SIBTF). The California SIBTF is a special fund administered by California's workers' compensation program to provide additional compensation to injured workers who already had a disability or impairment at the time of a subsequent injury.

Beginning in 2016, Do began to work for Liberty Medical Group Inc., a Rancho Cucamonga-based medical company, for which he would draft SIBTF-related medical reports that Liberty would then bill to the California SIBTF program. In October 2018, California suspended Do from participating in California's workers' compensation program, which included the SIBTF, because he had previously been convicted of federal health care fraud in 2003. Despite his suspension, Do continued to work for Liberty on SIBTF-related workers' compensation matters.

Do continued to perform similar actions for Liberty that he had been doing before his October 2018 suspension, including compiling and editing reports related to the SIBTF program.

To conceal that Do was unlawfully continuing to participate in the workers' compensation SIBTF program after his suspension, Liberty's owner came up with a plan. That plan was that Do would continue to author the SIBTF-related reports, which Liberty would then continue to mail to the California SIBTF for payment.

Rather than listing Do's name on the billing forms and the attached medical reports mailed to the California SIBTF, like they had had done before Do's suspension, Liberty instead fraudulently listed other doctors' names on the billing forms and attached medical reports, even though Do had drafted and compiled the reports. Do admitted that Liberty was paid more than \$3 million by California SIBTF for such reports that Liberty mailed to the California SIBTF for payment after Do's October 2018 suspension.

Do's plea agreement also details that Liberty's owner edited Do's medical reports, even though that co-conspirator was not a doctor or other licensed medical professional. ([Source](#))

Former Chairman Of Health Care Company Board of Directors Sentenced To Prison For [Selling \\$1.3 BILLION+ Of Unregistered Securities](#) - December 4, 2024

Avtar Dhillon is the former chairman of Massachusetts-based company Arch Therapeutics, Inc.

He was sentenced to prison for three felony securities offenses, two of which concerned his undisclosed sale of over \$1.3 million worth of company shares.

Dhillon and his then attorney, Daniel Martinez, placed 2.75 million Arch Therapeutics shares that Dhillon beneficially owned into a limited liability company that Martinez created.

Dhillon and Martinez then worked together to sell the shares in the open market without a valid exemption under the relevant securities laws and to distribute the approximately \$1.34 million in proceeds.

The proceeds were distributed primarily to third parties for Dhillon's benefit, with a small portion distributed to Martinez directly. Dhillon thereafter willfully failed to report the stock sales to the U.S. Securities & Exchange Commission and the investing public, as he was required to do. ([Source](#))

Account Manager For Dermatology Clinic Sentenced To Prison For [Stealing \\$715,000+ / Used Funds To Pay Credit Cards Debt](#) - November 27, 2024

Between May 2020 and March 2023, Carol Casilla was employed as an accountant by Spokane Dermatology Clinic (SDC), a dermatological practice located in Spokane.

While employed at SDC, Casilla used her position to fraudulently issue company checks to herself and deposit them into her own personal accounts, and to make electronic funds transfers using company funds toward her personal credit cards.

According to court documents, some of the transfers were made to a fictitious company that Casilla created in order to make it appear as though the transfers were for legitimate company expenditures. Casilla made hundreds of fraudulent transfers in this manner, stealing more than \$715,000 in total. ([Source](#))

Medical Center Employee Sentenced To Probation For Criminal Abuse Of A Vulnerable Adult - December 10, 2024

Eleano Flowers was employed as a Patient Sitter at United Medical Center, a hospital in Southeast Washington.

On January 4, 2021, while attempting to change the soiled clothing of a 68-year-old patient under her care, Flowers struck the patient repeatedly with the hospital bed's remote controller.

The victim, who had previously suffered a stroke, was paralyzed on one side of his body, unable to speak, and classified as a "vulnerable adult" under D.C. Code § 22-932.

The assault was captured on cellphone video by another Patient Sitter in the room, who witnessed the abuse. The video showed Flowers' repeated strikes, causing visible distress to the victim. Flowers was terminated from her position following the incident, which was reported to hospital authorities and subsequently investigated by the D.C. Office of Inspector General. ([Source](#))

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

Cryptocurrency Firm Vice President Sentenced To Prison For **Stealing \$4.4 Million+ From Employer - December 17, 2024**

Dylan Meissner was employed at a cryptocurrency research firm as Vice President of Finance with access to the firm's cryptocurrency wallets and bank accounts.

In approximately January 2022, Meissner obtained a 50 Ethereum (approximately \$170,000) loan from his employer, stating that he would use the funds in an attempt to avoid a substantial loss in certain cryptocurrency investments he had made using his personal funds. Then, from February 2022 until his termination in November 2022, in continued attempts to counteract significant personal trading losses, Meissner fraudulently diverted his employer's funds to his own use and covered up his conduct through false entries in the firm's books and records.

Through this scheme, Meissner stole approximately \$4,461,828 from his employer. ([Source](#))

Chief Financial Officer Admits **Stealing \$1.3 Million+ From 2 Law Firms He Was Employed By - December 11, 2024**

Tony Archuleta-Perkins, held various roles at the firms, eventually becoming Chief Financial Officer (CFO). As the CFO, Archuleta-Perkins was in a position of trust and had access to the law firms' payroll systems and end-to-end payments automation platforms.

During the course of his employment, Archuleta-Perkins used this access to embezzle funds in various ways.

The primary way that Archuleta-Perkins stole money from the law firms was to cause the firms to make false and fraudulent payments to a non-profit organization he had set up and solely controlled. Archuleta-Perkins admitted to stealing more than \$1.1 million using this method.

Archuleta-Perkins also embezzled funds from the law firms by falsely adding "one-time reimbursements" to his regular paychecks or special bonus payroll checks through the use of the law firms' payroll software. He admitted to stealing more than \$106,000 using this method. Archuleta-Perkins also admitted that he endorsed a \$41,663.69 tax refund check made out to one of the law firms, deposited it into a bank account belonging to the non-profit, and then wrote himself a check for the same amount.

In total, Archuleta-Perkins admitted that he was responsible for at least \$1,321,752.72 in losses to his victims. Archuleta-Perkins used the stolen money for personal expenses, including payments on a Best Buy credit card. ([Source](#))

Mortgage Title Company Employee Admits To Orchestrating \$350,000+ Real Estate Wire Fraud Scheme - December 20, 2024

Mayela Cantu admitted she knowingly participated in a scheme that used falsified lien payoff statements, fraudulent warranty deeds and deceptive emails to mislead lenders, title companies and property buyers.

From November 2020 until her arrest, Cantu defrauded buyers and lenders in multiple property transactions while working at Sierra Title in McAllenm Texas. Using her position of trust, she facilitated closings backed by falsified documents. In one notable case, she directed others to create a fraudulent email address resembling that of a legitimate lienholder. Cantu then used the fake account to send false payoff amounts via interstate wires, leading a title company to improperly disburse more than \$350,000.

Cantu facilitated additional fraudulent property transactions, including arranging closing on properties that had already been sold and accepting undisclosed cash payments. By concealing the true nature of these deals, she caused significant financial harm to the affected parties. ([Source](#))

Employee Sentenced To Prison For Embezzling \$116,000 - December 13, 2024

Angela Mitchell embezzled approximately \$116,998.70 from Company A by fraudulently transferring funds from Company A's bank accounts via electronic transfers and by drafting unauthorized checks to herself.

Mitchell committed the fraud during her employment, and continued illegally accessing Company A's accounts after she was terminated in June 2018. ([Source](#))

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMENT AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

Human Resource / General Manager Charged With \$1.5 Million Of Fraud / Used Funds To Pay Credit Card Bills, Trips, Etc. - December 26, 2024

In 2008, James Wohlers was hired by GBR Equipment/Oilfield Services (GBR), an Anchorage, Alaska based business that provides oilfield services on the North Slope and elsewhere, as their human resource manager. In 2009, Wohlers became their general manager, overseeing vendor interface, employee hiring, payroll and accounting. Part of his responsibilities included coordinating wire transfers from GBR's bank account to outside accounts.

In 2019, an audit was completed on the company's finances and bank records after employees determined the company was earning sufficient revenue but was unable to pay vendors and employees. The audit revealed that from at least 2013 to 2019, Wohlers allegedly executed wire transfers from the GBR account that did not benefit the company, and allegedly used GBR's corporate credit cards for personal expenses, like paying personal credit card bills.

The indictment alleges that in 2015, Wohlers formed a partnership named BGI Industrial Services (BGI), which was registered with the Alabama Secretary of State. In 2017, GBR performed services for two companies. Wohlers allegedly sent both companies invoices from BGI for \$25,000 and \$2,500 respectively, and both companies paid the invoices. The money was deposited into BGI's bank account.

Wohlers also allegedly used GBR credit cards to pay for business expenses related to BGI and used employees paid by GBR to complete work on behalf of BGI.

In late 2015, Wohlers announced GBR employee pay cuts of 5 to 10 percent, along with other restrictive measures to address GBR's poor financial condition. A few months later, Wohlers announced additional GBR employee pay cuts of 5 to 15 percent. Within two weeks of making his second announcement, Wohlers allegedly used over \$43,000 of GBR's funds to pay for airfare and other expenses related to a personal trip to China.

Wohlers was terminated by GBR in August 2019, and the company sent the defendant a demand letter stating he owed GBR \$1.5 million. After being terminated, Wohlers allegedly deleted roughly 10,000 emails from GBR's servers. ([Source](#))

Factory Environmental Manager Sentenced To Prison For [Stealing \\$1.2 Million+ To Profit His Company, Pay For Hunting Trips, Etc.](#) - August 22, 2024

Around early December 2016, Michael Mayfield was employed as an environmental manager at the Mars Wrigley factory in Flowery Branch, Georgia. In that role, he oversaw the Health, Safety, and Environmental and Recycling Programs.

The recycling waste produced at the factory was valuable and companies often made direct payments or sent Mars Wrigley rebate checks after disposal of the material. But unbeknownst to Mars Wrigley, Mayfield diverted the checks to his own company, WWJ Recycling.

The fraudulently obtained checks totaled over \$500,000. Mayfield used the funds to pay for hunting trips worth more than \$100,000, a donation to his church for more than \$80,000, and more than \$200,000 in personal checks.

Mayfield also directed his co-conspirator to create false invoices from ASA Safety Supply, a supplier to Mars Wrigley.

The co-conspirator sent the invoiced items to Mayfield for his personal use and then submitted false invoices from ASA Safety Supply to Mars Wrigley for payment. The purchased items included football supplies for the Flowery Branch High School football team, such as cleats and clothing, improvements to the stadium, tickets to a University of Georgia football game, and gift cards. These false invoices totaled over \$199,000.

Mayfield also sent invoices from WWJ Recycling to ASA Safety Supply. His co-conspirator directed ASA Safety Supply to pay those invoices and then submit the false invoices to Mars Wrigley for payment for work that was not done. The WWJ Recycle invoices totaled over \$750,000.

Mayfield engaged in this scheme from as early as December 2016 until sometime in 2022. Ultimately, Mars paid over \$1.2 million because of Mayfield's fraudulent scheme. ([Source](#))

Law Firm Office Manager Charged For [Embezzling \\$1.2 Million Dollars For Personal Use](#) - December 13, 2024

Catherine Daly was employed by a local law firm in Tennessee as its office manager. As office manager, she had access to the firm's bank accounts, including the firm's operating account, which was used to pay the firm's operating expenses. The operating account was both opened and located at a Memphis branch of what was then known as SunTrust Bank.

Daly had two American Express (AmEx) charge accounts in her name with a total of five AmEx charge cards issued through the two accounts to Daly and two of her relatives.

The cards were used to purchase various goods and services such as clothing, shoes, designer handbags, and jewelry; fixtures and furnishings for Daly's residence; food purchased at restaurants; personal services at nail and beauty salons; and travel expenses.

Daly is alleged to have used the money in the firm's operating account to pay the amounts due on her personal AmEx charge accounts. She conducted the embezzlement scheme from June 2019 until October 2021, allegedly making multiple payments on her personal AmEx bills directly from the law firm's operating account. Using this method, Daly embezzled and converted \$1,289,085.00 of the law firm's funds to her own use.

([Source](#))

Chief Financial Officer Sentenced To Prison For [Misappropriating \\$1 Million+ Of Company Funds For His Own Benefit](#) - December 5, 2024

Jon Rush was employed first as the Vice President, and subsequently Chief Financial Officer, of a logistics and transportation company. The company arranges for the transportation of freight and cargo for the military, defense contractors, disaster relief organizations, and others.

From 2016 to 2020, Rush misappropriated the company's funds for his own benefit and misdirected funds to pay off his debt.

As part of the scheme Rush transferred funds from the company's bank accounts to bank accounts he owned or controlled, then he recorded these transfers in the company's internal accounting software to conceal the fraud. Rush disguised the monetary transfers by using the names of vendors with whom company routinely did business.

Jon Rush was ordered to pay \$1,062,459.49 in restitution to his victims. ([Source](#))

Real Estate Agency Employees Pleads Guilty To [Embezzling \\$1 Million+ / Used Funds For Vacations, Luxury Fashion & Taylor Swift Tickets](#) - December 19, 2024

Between January 2020 and November 2023, Jennifer Tinker defrauded a real estate agency that she worked for by transferring more than \$1 million of company funds through wire transfers, Zelle payments, checks, and ACH to her personal bank accounts. Tinker fraudulently embezzled funds from the real estate agency's accounts – including its escrow, operating, and commission accounts.

Tinker hid the transfers by listing fictitious "recipients" on the wire transfer paperwork to make them appear legitimate. She then wired the stolen funds into her personal bank accounts. Between approximately February 2021 and November 2023, Tinker wired money to her personal accounts more than 90 times. Additionally, Tinker made false and fraudulent edits and entries into her employer's internal accounting records to conceal the transfers.

The defendant used the funds that she stole from her employer to pay for luxury goods and personal expenditures such as vacations, Taylor Swift tickets, and five different vehicles. ([Source](#))

Employee Pleads Guilty To [Embezzling \\$650,000+ / Spent Money On Private Jets, Etc.](#) - December 13, 2024

The schemes began in 2019, Westcot when Francis-Curley embezzled money from his then-employer by misusing cloud computing resources and accounts available to him as an employee. Francis-Curley used employer bank accounts and his employee work authorizations to purchase cloud computing resources, then sell them back to the company—paying himself with company money—at many times their market value. Through this scheme he obtained more than \$550,000, and he was caught while attempting to obtain another half-million dollars. He spent significant portions of the proceeds on extravagances, such as private jets.

In 2020, Francis-Curley defrauded the Paycheck Protection Program, a COVID assistance program designed to help small businesses and their employees weather the pandemic. Francis-Curley filed paperwork claiming that two companies he controlled had large payrolls that qualified for assistance, when in fact they had no operations, had no payroll, and did not qualify for relief. He obtained nearly \$100,000 and spent much of it on personal goods and services.

Finally, in October 2022, Francis-Curley applied for and obtained a credit card in the name of his former significant other. Francis-Curley used the card for more than \$1,000 in personal expenditures. ([Source](#))

Bar Association Executive Director Sentenced To Prison For [Stealing \\$200,000 To Fund Personal PayPal Account](#) - December 13, 2024

From January 2019 to August 2023, Peonie Cabrera served as the Executive Director of the Northern Mariana Bar Association (NMBA), in the Mariana Islands.

Her duties included managing membership fees for the office. During that time, she diverted over \$200,000 of NMBA funds through federally insured bank accounts for personal use. She presented fraudulent payroll documents and paychecks for signature by NMBA board members. These were drawn upon NMBA's bank account and made payable to Cabrera. She also withdrew cash from NMBA's savings account for personal use on 13 occasions.

She further used NMBA's bank accounts to make over 150 payments to her PayPal account for personal use. During 2020 through 2023, Cabrera also diverted payments from NMBA members via other electronic payment accounts for her personal use. ([Source](#))

Employee Pleads Guilty To Using Company Credit Card And [Spending \\$100,000 For Rent, Wedding Reception, Etc.](#) - December 5, 2024

From June 2015 to February 2023, Brandon Thompson was an administrator with a Virginia joint venture among physicians in conjunction with Sentara Hospital. Thompson's responsibilities included purchasing equipment, implementing capital and operating budgets, and promoting cost containment and efficient use of facility resources.

From at least January 2018 through February 2023, Thompson used a company card for, among other things, his rent, wedding reception, divorce attorney, and groceries. He also used the card for such luxury items as diamonds, airline tickets, and an initiation fee for a country club membership.

Thompson is scheduled to be sentenced on May 9, 2025, and faces up to 20 years in prison. Actual sentences for federal crimes are typically less than the maximum penalties. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors. ([Source](#))

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Bookkeeper And Sister Sentenced To Prison For [Embezzling \\$1.5M](#) From Business - December 5, 2024

Margaret Heilman was the bookkeeper for a business in Florence County. As bookkeeper, she had access to the business's bank accounts and had signature authority.

Beginning in 2014, Heilman began to write checks to herself and others, to include her sister, Gray, for personal expenses. When Heilman wrote the checks to herself, and others, she made them look like legitimate business expenses on the business's general ledger.

Through the course of the scheme, Heilman defrauded the company out of \$1.5 million. ([Source](#))

Company Manager Charged With [Stealing \\$1.3 Million Using Fake Invoices Scheme](#) - December 2, 2024

John Laakso worked as a contractor, and later as engineering manager, with GAF Materials Corporation. One of his duties was to procure equipment and services for the GAF facility in Savannah, Georgia.

From 2021 to 2023, Laakso assumed fictitious personas and created pass-through companies, hiding these activities from GAF.

He would award contracts to those fictitious companies which, in turn, would subcontract with an actual vendor to provide the product or service at a lower cost. Laakso would then keep the difference in price for his own use and enjoyment.

The scheme resulted in GAF paying more than \$1.3 million in fraudulent invoices, with Laakso keeping hundreds of thousands for himself from the marked-up costs. ([Source](#))

Employee Sentenced To Prison For [Embezzling \\$1 Million+](#) By Creating A Fake Company - December 12, 2024

Between 2017 and 2023, Brandon Alford was employed as a service writer for a heavy equipment supplier located in Indiana. In this role, he acted as a liaison between customers and service providers, one of which was a machine parts retailer located in Indiana that occasionally sold parts to Alford's employer.

In 2017, Alford devised a scheme to defraud his employer by creating a fake company, A&D Distributing LLC.

He convinced a manager at the retailer to sell machine parts to his employer through A&D Distributing, positioning the retailer as a middleman. Alford claimed he would handle all logistics, including shipping the parts to his employer, while the retailer would simply invoice the employer for the parts, plus a profit margin.

Between December 2017 and January 2023, Alford submitted 25 fraudulent invoices to the retailer for parts that were never ordered or delivered. The retailer paid Alford \$939,500 through 22 wire transfers to A&D Distributing's account. The retailer then invoiced Alford's employer based on these false invoices, resulting in the employer paying a total of \$1,006,500 for non-existent parts.

Alford exploited his position at the company where he worked to ensure the fraudulent invoices were approved and paid, despite no parts ever being delivered. ([Source](#))

Operations Manager For Convention Center Charged With [Pocketing \\$26,000+ In Kickbacks From Vendor](#) - December 4, 2024

An operations manager at McCormick Place Convention Center in Chicago has been indicted on federal fraud charges for allegedly pocketing kickbacks from a company contracted to provide snowplow services at the facility.

Dominick Gironda was employed on behalf of the Metropolitan Pier and Exposition Authority, which operates McCormick Place.

Gironda managed contracts with vendors that provided services at the McCormick Place campus, which consists of multiple buildings, parking lots, and other spaces for conventions and trade shows. Gironda schemed with an associate, James Sansone, to approve inflated invoices for services that were not actually provided at McCormick Place. The false invoices included compensation for individuals who had not worked on particular snow removal projects and equipment that had not been utilized, the indictment states.

After Gironda approved full payment of the false invoices, cash was kicked back to Sansone, who then passed on some or all of the money to Gironda, the indictment states.

From 2022 to earlier this year, Gironda and Sansone allegedly received kickbacks totaling approximately \$26,700. The indictment alleges that when Gironda, Sansone, and others texted with each other about the scam, they used coded language that referred to the kickback payments as bottles of wine. ([Source](#))

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

ByteDance Seeks [\\$1.1 Million In Damages](#) From Employee Who Sabotaged AI Project - November 28, 2024

ByteDance, the owner of TikTok filed a lawsuit against a former intern, accusing him of tampering with code and sabotaging an artificial intelligence (AI) training project and demanding \$1.1 million in compensation as well as a public apology.

ByteDance identified the intern, surnamed Tian, as having acted out of dissatisfaction with the team's resource allocation.

Tian tampered with code to disrupt a research project's model training work, causing significant waste of resources. The company said it reported Tian's actions to two professional ethics organisations in China, the Trust and Integrity Enterprise Alliance and the Enterprise Anti-Fraud Alliance, as well as to Tian's university.

Despite these measures, the former intern repeatedly denied any wrongdoing during the investigations, leading the company to pursue legal action. ([Source](#))

THEFT OF ORGANIZATIONS ASSETS

Luxury Jewelry Company Supervisor Sentenced To Prison For Stealing& Selling \$1.7 Million+ Worth Of Precious Metals - December 4, 2024

From 2018 until early 2024, Benjamin Preacher worked as a manufacturing supervisor at a Rhode Island facility operated by a company that sells luxury items, including jewelry made from gold, silver and platinum.

Preacher used his position overseeing the production and security of high-end jewelry to steal scrap precious metals from the company's facility in Rhode Island. Preacher then drove the stolen metals into Massachusetts and then sold them to various businesses in Massachusetts.

Preacher stole over \$1.7 million in gold, silver and platinum from his employer over a period of more than three years. ([Source](#))

EMPLOYEE COLLUSION (WORKING WITH INTERNAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Emergency Medical Technician Sentenced To Prison For Drug Tampering - December 5, 2024

Cleola Hogan was working her shift as an Emergency Medical Technician (EMT) on March 20, 2022, when she removed Benadryl from a vial using a syringe and injected the Benadryl into her arm.

Hogan then replaced the missing Benadryl with saline solution and glued the cap back onto the Benadryl vial. Benadryl is commonly used to treat patients with severe allergic reactions, and replacing Benadryl with saline would place patients who needed Benadryl at risk of death or serious bodily injury. ([Source](#))

Nurse Pleads Guilty To Opioid Diversion Scheme - December 12, 2024

Jacqueline Brewster admitted that she unlawfully accessed and used individually identifiable health information of patients at Raleigh General Hospital in Beckley, West Virginia to divert hydromorphone, an opioid, for her personal use. Brewster was employed as a travel nurse at Raleigh General Hospital from September 2021 until February 2022.

To carry out her diversion scheme, Brewster accessed automated controlled substance dispensing machines at Raleigh General Hospital using her personal biometrics and began the process for checking out hydromorphone purportedly for a patient. Once the machine's drawer opened, Brewster siphoned off a portion of hydromorphone from its vial, diluted the remaining hydromorphone with another substance so the vial would appear full, reattached the cap and returned the vial to the machine drawer. She subsequently canceled the transaction.

Brewster admitted that on one occasion she unlawfully accessed individually identifiable health information and obtained a hydromorphone by fraud occurred on or about February 1, 2022, at Raleigh General Hospital.

Brewster further admitted that she carried out her scheme and diverted hydromorphone many times over the course of her employment at Raleigh General Hospital, and that she siphoned the hydromorphone not for any legitimate use. ([Source](#))

Hospital Nurse Pleads Guilty To Illegally Obtaining Fentanyl From Hospital - December 16, 2024

Charles Welch, was a certified registered nurse anesthetist at Lake Ozark Anesthesia in Missouri. He primarily provided anesthesia services at Lake Regional Hospital in Osage Beach. Welch was responsible for preparing various medications for use in daily medical procedures.

Welch admitted that he stole fentanyl from the automated dispensing cabinets located in the hospital's operating rooms from approximately July 1 through Aug. 21, 2023.

Welch specifically pleaded guilty to fraudulently obtaining a vial of fentanyl which was for use in a medical procedure, by scanning the fentanyl to generate a label that Welch affixed to a syringe he had previously filled with saline, thus concealing the true contents of the syringe and enabling Welch to divert the fentanyl for his 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

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

No Incidents To Report

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS

<https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html>



DEFINITIONS OF INSIDER THREATS

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](#) & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

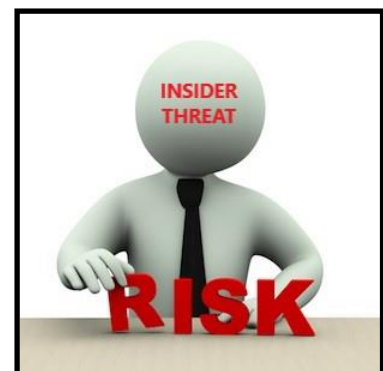
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

ORGANIZATIONS IMPACTED

TYPES OF ORGANIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of \$\$\$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction & Downtime
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead



Reputation Impact

- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees'

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business





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

BILLIONAIRE LIFESTYLE



INSIDER THREATS

Employees' Living The Life Of Luxury Using Their Employers Money

NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

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 By Bribed Employees / 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+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over \$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 prison for conspiring to launder BILLIONS of dollars embezzled from 1Malaysia Development Berhad (1MDB), conspiring to violate the Foreign Corrupt Practices Act (FCPA) by paying more than \$1.6 BILLION in bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

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

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

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

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

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

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

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

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

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

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

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

2 Former Employees Of Mortgage Lending Business Charged For Roles In \$1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo’s assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain properties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than \$1.4 billion in loans. ([Source](#))

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

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

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

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

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

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

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

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

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

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

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

COLLUSION – HOW MANY EMPLOYEES’ OR INDIVIDUALS CAN BE INVOLVED?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 Individuals (Hospital Managers And Others) Charged In \$1.4 BILLION Hospital Pass - Through 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](#))

Former 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](#))

Former 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

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](#))

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

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

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

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, 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 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](#))

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

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

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

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

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

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

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

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

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

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

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

Former 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 & Obez, 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 & Obez's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obez's largest customer, Giant Food. Worley & Obez 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](#))

Former 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](#))

Former 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](#))

Former 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

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

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](#))

Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022

Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

On or around June 21, 2022 a 55 year old female coworker of Ortiz, experienced a medical emergency and died immediately after treating herself for dehydration using an IV bag of saline taken from the surgical center. An autopsy report revealed that she died from a lethal dose of bupivacaine, a nerve blocking agent.

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU.

Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupivacaine, and lidocaine.

Surgical center personnel concluded that the incidents listed above suggested a pattern of intentional adulteration of IV bags used at the surgical center. They identified about 10 additional unexpected cardiac emergencies that occurred during otherwise unremarkable surgeries between May and August 2022 .

The complaint alleges that none of the cardiac incidents occurred during Dr. Ortiz's surgeries, and that they began just two days after Dr. Ortiz was notified of a disciplinary inquiry stemming from an incident during which he allegedly "deviated from the standard of care" during an anesthesia procedure when a patient experienced a medical emergency. The complaint alleges that all of the incidents occurred around the time Dr. Ortiz performed services at the facility, and no incidents occurred while Dr. Ortiz was on vacation.

The complaint further alleges that Dr. Ortiz had a history of disciplinary actions against him, and he had expressed his concern to other physicians over disciplinary action at the facility, and complained the center was trying to "crucify" him.

A nurse who worked on one of Dr. Ortiz's surgeries told law enforcement that Dr. Ortiz refused to use an IV bag she retrieved from the warmer, physically waving the bag off.

A surveillance video from the center's operating room hallway showed Dr. Ortiz placing IV bags into the stainless-steel bag warmer shortly before other doctors' patients experienced cardiac emergencies.

The complaint alleges that in one instance captured in the surveillance video, Dr. Ortiz was observed walking quickly from an operating room to the bag warmer, placing a single IV bag inside, visually scanning the empty hallway, and quickly walking away. Just over an hour later, according to the complaint, a 56-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. The complaint alleges that in another instance, agents observed Dr. Ortiz exit his operating room carrying an IV bag concealed in what appeared to be a paper folder, swap the bag with another bag from the warmer, and walk away. Roughly half an hour later, a 54-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. ([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](#))

Former 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 eighth victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

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

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

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

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

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

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

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

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

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

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

Former 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](#))

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>

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

CTTP = [China Thousand Talents Plan](#)

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

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

Protect America's Competitive Advantage

High-Priority Technologies Identified in China's National Policies

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

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

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






SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

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 (**5,900+ 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 MONTHLY REPORTS

July 2021 To Present

<http://www.insiderthreatincidents.com> or

<https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html>

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.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)

<https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf>

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

<https://www.insiderthreatdefense.us/category/insider-threat-incidents/>

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.

<https://www.insiderthreatdefense.us/news/>

INSIDER THREAT INCIDENTS COSTING \$1 MILLION TO \$1 BILLION +

<https://www.linkedin.com/post/edit/6696456113925230592/>

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

<https://twitter.com/InsiderThreatDG>

Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

<https://www.nationalinsiderthreatsig.org/critical-infrastructure-insider-threats.html>



National Insider Threat Special Interest Group (NITSIG)

*U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals*

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 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.

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:

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management 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
- ✓ Insider Threat Awareness Training
- ✓ 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. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal **FREE OF CHARGE**. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.

<http://www.nationalinsiderthreatsig.org/nitsigmeetings.html>

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 will also enable 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>

NATIONAL INSIDER THREAT SPECIAL INTEREST GROUP
INSIDER THREAT SYMPOSIUM & EXPO (TM)
March 4, 2025

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland

Are you looking for expert guidance from Insider Risk Management (IRM) Program Experts for developing, managing, evaluating or optimizing a program?

The NITSIG will be holding the Insider Threat Symposium & Expo (ITS&E) on March 4, 2025, at the Johns Hopkins University Applied Physics Laboratory (JHU-APL, Laurel, Maryland), in the Kossiakoff Center. The event runs from 8AM to 5PM.

This will be the 5th ITS&E held. Attendance numbers range between 250 to 500 people for these events.

This year's event will feature subject matter experts with real world experience in IRM Programs and an interactive breakout panel that will discuss a variety of IRM topics.

Confirmed Speakers

- Larry Knutsen / Retired CIA Insider Threat Program Manager
- Shawn Thompson / IRM Program Legal Expert (Former DoD Senior Litigation Attorney, FBI Assistant General Council)
- Todd Masse & Bill Smith / JHU- APL IRM Program
- Kevin Burton / Vice President, IRM Lead At Synchrony Financial
- Frank Greitzer, PhD / Chief Behavioral Scientist For Cogility Software
- Zak Lewis / EchoMark Insider Threat Leak Detection Tool
- Cyber Security & Infrastructure Security Agency (CISA)
- Deidra Bass / Director, Navy Insider Threat Program
- Department Of Defense Insider Threat Management Analysis Center (DITMAC)
- And More...

More Information Can Be Found On This Link:

www.insiderthreatsymposium.org

The ITS&E brings together individuals from the U.S. Government, Department Of Defense, Intelligence Community Agencies, Defense Contractors, Critical Infrastructure, Law Enforcement, Universities and the private sector companies, for a 1 day event that features expert speakers, engaging and interactive panel discussions, vendor technologies and solutions, and networking with IRM practitioners.

The expo will provide attendees with visibility into proven technologies and services for Insider Threat Detection and IRM. Vendors that are interested in exhibiting at this event, please see the link below.

<https://www.eventbrite.com/e/insider-threat-symposium-expo-3-4-25-vendor-registration-tickets-1069852169639>

The link below provides a complete overview of the NITSIG, advisory board members and the very positive comments (Page 19) from our membership and other individuals that have attended NITSIG meetings, workshops and ITS&E events.

<https://www.nationalinsiderthreatsig.org/pdfs/NITSIG%20Overview%20With%20Comments.pdf>

ITS&E Registration (Cost: \$69 – Early Bird Repristration (Includes Continental Breakfast / Lunch)

<https://www.eventbrite.com/e/insider-threat-symposium-expo-3-4-25-registration-tickets-1078741698459>

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and [exceptional satisfaction](#).

The ITDG offers the most affordable, comprehensive and practical [training courses](#) and [consulting services](#) to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and Insider Risk Management Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive Insider Risk Management. We will provide the training, guidance and resources to ensure that the Insider Risk Program Manager and key stakeholders are universally aligned from an enterprise / holistic perspective to detect and mitigate Insider Risks and Threats.

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training & Workshops For C-Suite, Insider Risk Program Manager / Working Group, Insider Threat Analysts & Investigators
- ✓ IRM Program Development, Management & Optimization Training & Related Courses
- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ 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

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verizon, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **675+** organizations. ([Client Listing](#))

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSIG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

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.

Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor

Insider Risk / Threat Vulnerability Assessment Specialist

ITP Gap Analysis / Evaluation & Optimization Expert

[LinkedIn ITDG Company Profile](#)

Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group

Founder / Director Of Insider Threat Symposium & Expo

Insider Threat Researcher / Speaker

FBI InfraGard Members

[LinkedIn NITSIG Group](#)

Contact Information

561-809-6800

www.insiderthreatdefensegroup.com

jimhenderson@insiderthreatdefensegroup.com

www.nationalinsiderthreatsig.org

jimhenderson@nationalinsiderthreatsig.org