INSIDER THREAT INCIDENTS REPORT

On

Personal Enrichment Schemes

By Employees

November 2025

Produced By

National Insider Threat Special Interest Group

Insider Threat Defense Group

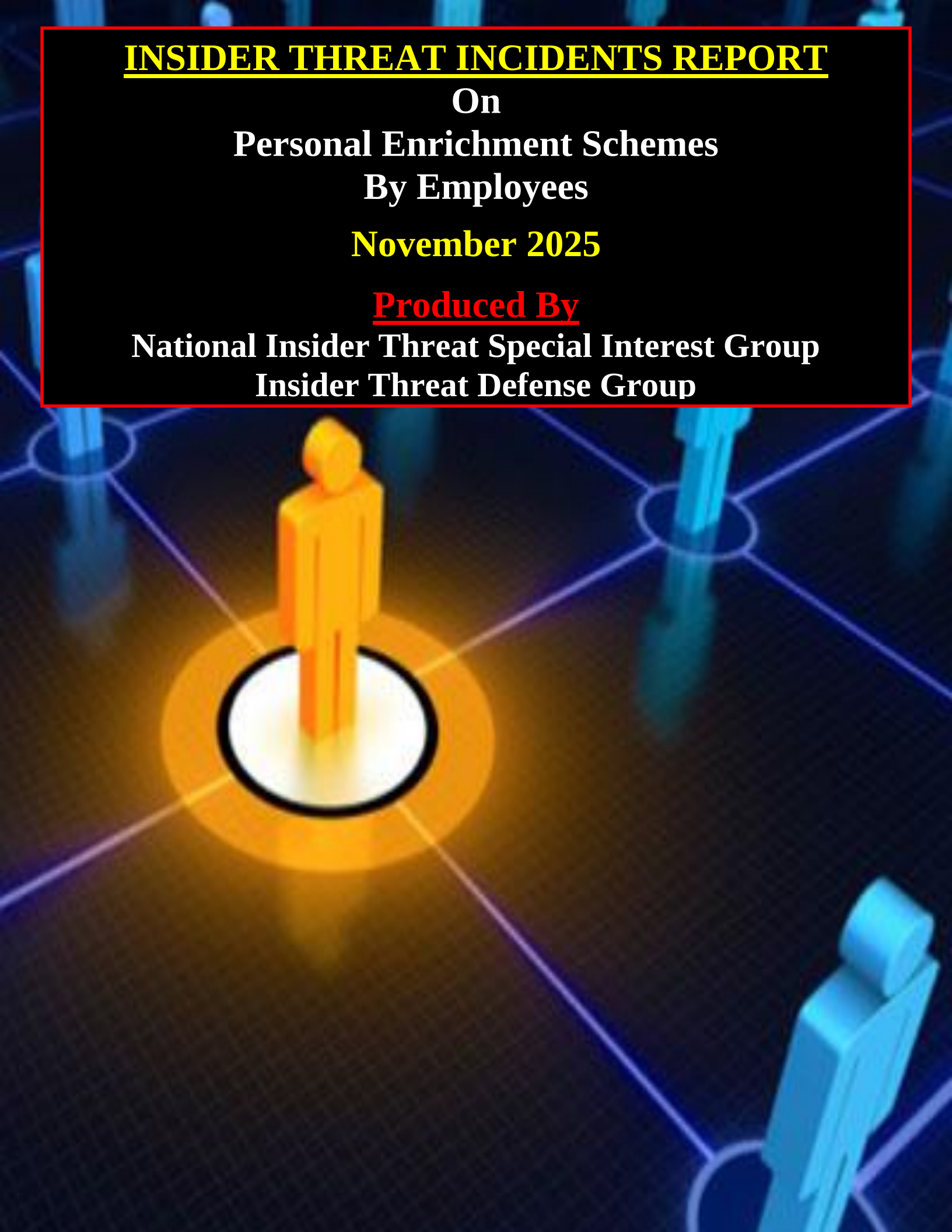


TABLE OF CONTENTS

EMPLOYEE PERSONAL ENRICHMENT SCHEMES OVERVIEW

OVERVIEW

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

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

In some cases a malicious employee might not being working alone. Employees might be in collusion with other employees, or employees might be in collusion with individuals external to an organization.

The traditional mindset that an employee will display observable behavioral indicators, may not be the case if the employee is not disgruntled. The employee may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay child support or pay medical bills, or need money to support their gambling problems, etc.

An employee, who is successful in stealing steal from their employer, will take advantage of opportunities (Lack Of Security Controls, Vulnerabilities) within an organization to achieve their desired malicious objectives.

According to the Association of Certified Fraud Examiners (ACFE) 2024 Report On Fraud, 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.

The ACFE 2024 Fraud Report also states that providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. The report states 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**.

Comprehensive and robust Insider Risk Management (IRM) **MUST EXCEED** security compliance regulations and requires "Thinking Outside The Box" as the employees did as referenced in this report.

If key stakeholders supporting an organization's IRM Program are not **UNIVERSALLY ALIGNED** and collaborating from an enterprise / holistic perspective to identify, prevent or mitigate employee risks / threats, this can result in many of the problems as referenced in this report. A comprehensive IRM Program involves key stakeholders understanding their roles, responsibilities and the many complexities and interconnected cross departmental components that are critical to the success of the program.

When there is a breakdown in the Employer - Employee Trust Relationship, and the employee behavioral indicator warning signs are downplayed, ignored or not shared with the IRM Program, this lack of action and engagement to address the employee risks or threats can further push the employees down the path of disgruntlement. This is often referred to as the Critical Pathway To Insider Risk.

The Employer - Employee Trust Relationship Breakdown can be described as a circle of trust / 2 way street. The employee trusts the employer to treat them fairly and compensate them for their work. The employer trusts the employee to perform their job responsibilities to maintain and advance the business.

When an employee feels this trust is breached, an employee may commit a malicious or other damaging action against an organization.

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 for the personal enrichment of the employee as this report will reveal.

Many times the malicious actions of employees are far more damaging than a data breach or ransomware attack caused by someone **EXTERNAL** to the organization.

This report covers the year 2025 and provides a snapshot of what employees do with the money they steal from their employers

The data for this report was gathered from research conducted by the National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG). The NITSIG and ITDG have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **6,700+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The Methods Of Employee Theft For Personal Enrichment Are Varied And Often Depend On The Employee's Role:

Asset Misappropriation:
The most common form of occupational fraud, involves theft of company cash, inventory, or other physical property by an employee.

Financial Statement Fraud:
An employee who intentionally misrepresents a company's financial condition by altering or creating fraudulent financial statements, documents and invoices.

Embezzlement:
An employee who misappropriates the use of company funds for unauthorized and fraudulent purposes.

Corruption:
An employee who misuses their influence in a business transaction to gain a personal benefit. This can include taking bribes or kickbacks from vendors in the form of money or gifts.

Payroll Fraud / Time Theft:
A range of schemes by an employee, such as adding fake employees to the payroll, increasing the salaries of employees without authorization, receiving compensation for hours not actually worked, receiving compensation for fraudulent overtime claims for hours not worked.

Data Theft:
An employee whose actions involve stealing proprietary company information, customer data, or trade secrets for personal benefit, bringing it to a new employer or selling it to a competitor.

EMPLOYEE PERSONAL ENRICHMENT INCIDENTS

Office Manager Pleads Guilty To Embezzling $1.7 Million+ By Forging Business Owner's Signature On Checks 500 Times Over 8 Years / Used Funds For Personal Enrichment - September 30, 2025

Tammy Barcus is the former office manager and bookkeeper for an Ocean City based home builder in Maryland.

Barcus admitted to embezzling at least $1,790,000 from her former employer. She forged a business owner's signature on business checks at least 500 times. Barcus then concealed the embezzlement from her employer and the Internal Revenue Service (IRS) by making false entries into the business' books and records.

From 2016 through 2024, Barcus used her position of trust to embezzle money by issuing more than 500 fraudulently authorized checks from the home builder's business bank account. Barcus forged the signature of one of the owners on the face of the business checks and then deposited the checks into bank accounts she controlled. She then used the money for her personal enrichment.

The former office manager and bookkeeper concealed the scheme by hiding the embezzled income from the IRS. She also made materially false and fraudulent edits and entries into the home builder's internal accounting records to cover up the fraudulent payments and commingled the embezzled funds into a bank account she controlled. (Source)

Company Manager Pleads Guilty To Stealing $1.6 Million From Customer Credit Accounts / Used Funds His Wedding, Vacation, Etc. - September 25, 2025

Tony Ream pleaded guilty to wire fraud committed in connection with his employment as a credit supervisor for a Long Island Company.

Over the course of four years, Ream sent wire transfers totaling approximately $1.6 million from the Company's bank account to a bank account that he controlled, and used those funds for his own personal gain. Ream spent the stolen funds on his wedding, luxury international vacations, and a failed restaurant venture in South Carolina. (Source)

Financial Director For Company Charged For Misappropriating $8.2 Million Over 10 Years To Fund His Personal Business - September 23, 2025

Jordan Khammar is charged with wire fraud and money laundering for his role in a decade-long scheme to defraud a multinational media, brand management, and consulting company and stealing over $8.2 million.

Khammar was hired as a financial consultant in 2006 by a multinational media, brand management, and consulting company (Company-1). He eventually became the company's Financial Director with access to and control over a wide range of its financial accounts and systems including those tied to banking, accounting, bookkeeping and payroll functions. Between January 2015 and May 2025, Khammar abused that access and control to engage in a scheme to defraud Company-1 out of millions of dollars. During the 10-year period, Khammar initiated over 300 fraudulent wire transactions, sending himself more than $8.2 million dollars from Company-1's bank account.

Khammar wired most of the stolen money to an account held in the name of Olive Tree Ventures, Inc. (Olive Tree), a company that he founded, owned, and controlled. From the Olive Tree account, Khammar dispersed a large portion of the funds to finance his independent business ventures including his media production company, Sideswipe Media, Inc. (Source)

Insurance Company Claims Adjuster Found Guilty Of Stealing $580,000+ / Used Funds For Designer Clothing, Jewelry, Etc. - September 19, 2025

Between March 2021 and February 2022, Octavias Owens defrauded his employer, a regional insurance company, out of more than $580,000.

Owens, who worked as a claims adjuster at the company, would reopen claims files that had already been settled and paid out. He would upload "comparative estimates" that he created to the claim files to make it look like additional work had been done. Owens would then cause checks to be issued on the claims to a shell company that he controlled that was disguised as a construction and roofing company. After the checks were issued, Owens would cash the checks at Orlando-area ATMs. He then used the proceeds for his own personal benefit, including to purchase designer clothing, jewelry, hotel rooms, vehicle accessories, and other luxury items. (Source)

Florida State Housing Authority Employee Pleads Guilty To Stealing $155,000+ Of Federal Funds / Used Funds For Personal Benefit - September 19, 2025

Thomas Hoffman was an employee of the Palatka Housing Authority (PHA), which received federal funds from the United States Department of Housing and Urban Development (HUD) to administer public housing programs in Palatka and neighboring municipalities. Hoffman was responsible for information technology and accounts payable.

During an audit of vendors in 2025, PHA identified an unapproved company called "Data Max," which had received approximately 48 fraudulently issued payments from PHA's general account between July 2023 and February 2025, totaling $155,706. A federal investigation determined that Hoffman owned and controlled Data Max and its corporate bank account, and that Hoffman had caused the fraudulent payments to be issued. The investigation showed that Hoffman used the funds for his personal benefit. Bank surveillance footage obtained by investigators showed Hoffman cashing PHA checks issued to Data Max on numerous occasions.
(Source)

Bank Executive Sentenced To Prison For Stealing $2.4 Million / Used Funds For Personal Expenses - September 18, 2025

Andrew Blassie served as the Executive Vice President for the Bank of O'Fallon in Illinois. He defrauded the bank out of $1,972,887.67 in a check kite scheme from September 2023 through September 2024 during his employment.

Blassie admitted to falsely inflating the balance of his personal checking account at the Bank of O'Fallon by depositing checks he knew to be backed by non-sufficient funds. He deposited checks with non-sufficient funds from four personal accounts at three other banks and one credit union into the Bank of O'Fallon account.

Blassie paid nearly $2.7 million for personal expenses from the falsely inflated account thus using funds belonging to the Bank of O'Fallon. As the former Executive Vice President, Blassie used his position to conceal his fraud from the Bank of O'Fallon by scrubbing his name and account number from suspected kiting reports.

Blassie was ordered to pay $2,461,887.67 in restitution. (Source)

Director Of Finance & Human Resources Sentenced To Prison For Stealing Nearly $540,000+ / Used Funds For Travel, Clothing, Rent Payments - September 18, 2025

Joelle Fouse was the manager / director of finance and human resources for Promise Community Homes, formerly known as Rainbow Village(RV) in Missouri from 2012 to 2023. RV is a charity that provides housing and resources for adults with intellectual and developmental disabilities. She was responsible for payroll, expense reimbursement and maintaining the charity's books and records.

Fouse caused 71 unauthorized payroll deposits totaling $139,810 and 181 unauthorized expense reimbursement payments totaling $407,186 to be made to her personal bank accounts. She also used the charity's credit card to make 184 unauthorized personal purchases totaling $133,210. Her theft, and the unauthorized payments, caused the charity to overpay payroll taxes by approximately $10,694. She pleaded guilty in April of 2025 to three felony counts of wire fraud.

Fouse used the money to pay for personal expenses for herself and relatives including travel, clothing, entertainment, restaurants and rent payments. To cover up her crimes, she created false financial reports, doctored receipts, made false entries in the charity's financial records and prevented the charity's officials from accessing records which would have disclosed her scheme. (Source)

U.S. State Department Budget Analyst Sentenced To Prison For Embezzling $650,000+ / Deposited Money Into Personal Accounts - September 18, 2025

Levita Ferrer admitted that she abused her signature authority over a State Department checking account between March 2022 and April 2024 while working as a Senior Budget Analyst in the State Department's Office of the Chief of Protocol.

Ferrer issued 60 checks payable to herself and three checks payable to another individual with whom she had a personal relationship. She printed and signed each check and then deposited all 63 checks, which totaled $657,347.50, into her personal checking and savings accounts.

Ferrer attempted to conceal her scheme by using a common QuickBooks account at the State Department. After entering her name as the payee on checks in QuickBooks and then printing them, she often changed the listed payee in QuickBooks from herself to an actual State Department vendor. As a result, anyone viewing those entries in the QuickBooks system did not see Ferrer's name as the payee on the checks unless they accessed an audit trail. (Source)

Law Firm Employee Embezzled $2.7 Million+ / Used Fund For Gambling - September 17, 2025

Destiny Combs was the Accounting Manager for a surrogacy agency and affiliated law firm.

Between February 2019 and June 2023, Combs embezzled approximately $2.72 million from the businesses. Combs's scheme was simple: she used personal credit cards to fund her gambling habit, then used company funds to pay her credit card bills. Combs stole the money to fuel her online gambling addiction. She made fraudulent entries in the companies' books to disguise her credit card payments as business expenses, and exploited the trust and autonomy her company gave her to go undetected. Over 52 months, Combs made approximately 292 payments from the company accounts to her personal American Express credit card, totaling $2,723,025. Combs gambled away most of the $2.7 million she stole. (Source)

Bank Employee Sentenced To Prison For Stealing $158,000+ From Customer Accounts / Used Funds For High Priced Technology Items & Gambling - September 16, 2025

Between January 2023 and March 2024, Dekoda Clark was employed as a Relationship Banker at a bank branch in Evansville, Indiana. During this time, Clark exploited his position to steal approximately $158,208.53 from customer accounts by making unauthorized cash withdrawals and issuing fraudulent debit cards.

Leveraging his access, Clark created debit cards linked to the checking accounts of five individuals and two businesses without their knowledge or consent. He then used these cards to make 17 purchases at various retailers, including Dicks Sporting Goods, Guitar Center, and Best Buy. Several of the purchases were for high-value technology items, including three Apple iPads, a MacBook Pro, an Apple Watch Ultra, two large televisions, a Lenovo gaming laptop, memory cards, a DJI Mini Drone, and an Xbox game drive. One of the transactions was for a $2,000 deposit into Clark's account with Draft Kings, an online sports betting platform. These fraudulent purchases totaled $15,708.53.

Clark also withdrew a total of $142,500 as cash from the checking accounts of three individuals without their knowledge or consent. (Source)

School Employee Sentenced To Prison For Embezzling $30,000+ From School District / Used Funds For Personal Benefit - September 16, 2025

Jonnie Eagle, while working for the Heart Butte School District, Montana, embezzled funds by using school credit cards and purchase orders, presenting such orders to local grocery stores, and obtaining and using gift cards for her own personal benefit, none of which was authorized. While doing so, Eagle forged the name of school employees to cover up the fraudulent transactions. (Source)

Employee For Non-Profit Sentenced To Prison For Embezzling $2.3 Million+ / Used funds For Remodeling Home, Mortgage, Credit Card & Car Payments - September 11, 2025

Marcia Joseph was a former senior fiscal officer for a non-profit organization.

Joseph admitted stealing $2,339,700 from the Non-Profit and funneled the funds to a sham company she had set up. The invoices described services purportedly provided in connection with a New York City Department of Education educational program focusing on students in shelters and, later, job training for adults in shelters. Over the course of nearly 17 years, Joseph generated and submitted more than 500 fictitious invoices and manipulated the Non-Profit's accounting systems to avoid detection. She used the stolen funds to pay for numerous personal expenses, including approximately $235,000 in mortgage payments, $207,000 in credit card payments, $98,000 in car payments, $45,000 in Amazon expenses, and various other personal items, such as home remodeling, spa treatment, landscaping expenses, and luxury goods. (Source)

Company Bookkeeper Pleads Guilty To Embezzling $860,000+ From 2 Different Employers / Used Funds For Personal Expenses - September 9, 2025

Fom mid-2018 to April 2022, Marie Higgins was employed as a bookkeeper for New England Kitchen & Bath LLC in Glastonbury.

Higgins stole from the business by issuing company checks payable to herself, often including the words "commission" or "bonus" in the memo line of the check, and used a signature handstamp of the company's owner to issue the checks; initiating wire transfers to bank accounts in her name; creating a fictitious supplier and billing the company for fictious expenses; using company debit cards to pay for personal expenses;

and overseeing a construction proposal for a legitimate client project, expensing incurred costs of the project through the company, and having the client pay her directly. Higgins stole $504,807 through this scheme.

From February 2023 to April 2024, Higgins was employed as an accounting manager for PVC Solutions, Inc., in Danbury, a company that produces and distributes PVC products. Higgins stole from the company by issuing company checks payable to herself; creating duplicate vendor payment templates to initiate wire transfers to her personal bank account; creating fictitious suppliers to bill the company on her behalf; and paying personal expenses through the company's bank account. Higgins manipulated the company's accounting records to conceal her criminal activity. Higgins stole $356,181 through this scheme. (Source)

2 Executives Sentenced To Prison For $1.9 Million Fraudulent Invoicing & Shell Company Scheme / Used Funds For Luxury Vehicles, Credit Card Payments, Etc. - September 8, 2025

From 2013 to 2020, Michael Vergato served as a vice president at Arrow Electronics, where he oversaw performance tuning of the company's Oracle EBS databases, including work performed by Mark Perlstein's company.

Vergato and Perlstein devised a scheme to bill the data management company for performance tuning services purportedly to be completed by a shell company created by Vergato, Oracle Performance Tuning and Optimization, LLC (OPTO). Posing as a legitimate contractor, OPTO submitted 21 fraudulent contracts and invoices to the data management company for database performance tuning services that were never performed. Perlstein, in his position as CEO, approved the invoices and wired payments to OPTO.

The scheme funneled nearly $2 million in company funds into OPTO. Perlstein and Vergato divided the proceeds, concealing their involvement by using personal email accounts, other corporate entities, and fake identities. To conceal his role, Vergato used his stepdaughter's identity to conduct business on behalf of OPTO. At trial, the data management company's current CEO testified that the company could not substantiate any work performed by OPTO or identify any actual employees or contractors related to that entity. Tax records confirmed OPTO paid no salaries and issued no contractor forms.

In total, the data management company paid OPTO $1,949,023. Of that amount, Vergato retained approximately $874,000, using the funds for luxury vehicles, credit card payments, retirement accounts, and rent. Perlstein personally received more than $1 million through the scheme. (Source)

Business Manager For Private School Pleads Guilty To Embezzling $239,000+ / Used Funds For Travel, Concerts, Rent, Etc. - September 4, 2025

From May 2021 through June 2024, Shannel Hilliard, 46, was the business manager for a private school in Richmond, Virginia. As business manager, Hilliard's responsibilities included management and maintenance of the school's books and records, performance of periodic bank reconciliation reports, and making purchases and payments on behalf of the school. As part of those responsibilities, Hilliard had control of a credit card in the school's name for official school business only.

From November 2021 through July 2024, Hilliard used the school's credit card to pay for personal expenses, including trips to Orlando, Las Vegas, Myrtle Beach, and Miami; performances such as Hamilton and concerts such as Usher, LL Cool J, and Capitol Jazz; luxury goods such as purses and jewelry; and rent for Hilliard's personal residence. On May 24, 2024, Hilliard used the credit card for a $1,591.77 payment to the Boathouse at Rocketts Landing for a personal graduation party.

Hilliard attempted to conceal her embezzlement by falsifying the school's bank reconciliation reports, including misrepresentations that certain expenses fell under categories of approved spending. For example, Hilliard attributed personal expenses such as a cruise on Royal Caribbean, a hotel stay in Winston-Salem, North Carolina, and a deposit to the Boathouse at Rocketts Landing to category for ongoing construction at the school. (Source)

U.S. Postal Worker Stripped Of Citizenship, Sentenced To Prison For Stealing $1.6 Million From U.S. Mail / Used Funds For Lavish Lifestyle, Strip Clubs, Etc. - September 3. 2025

Hachikosela Muchimba, 45, is a former letter carrier for the U.S. Postal Service.

Muchimba was stripped of his U.S. citizenship and to prison today in connection with mail theft and bank fraud scheme that illegally netted him $1.6 million.

Muchimba, originally of the Republic of Zambia, was naturalized as an American citizen on May 26, 2022. The mail theft and bank fraud scheme ran from December 2020 until March 2023. On his application for citizenship he falsely claimed to United States Citizenship and Immigration Services that he had not previously committed any criminal activity, all the while he was actively conducting his theft of mail and scheme to defraud. Because it was unlawfully procured, the Court revoked Muchimba's citizenship.

Between December 2020 and March 2023, Muchimba was a letter carrier based in Friendship Heights, when he executed a scheme to steal U.S. Treasury checks and private party checks from the U.S. mail. The stolen checks were intended for District postal customers living on over 30 different mail routes. Muchimba deposited the checks, sometimes while wearing his U.S. Postal uniform, into bank accounts under his control. Bank surveillance footage captured images of him making deposits and withdrawals of the funds.

The total amount of the U.S. Treasury checks fraudulently deposited into Muchimba's various bank accounts was over $1.6 million. Muchimba used the money to fund a lavish lifestyle that included international travel, stays at luxury hotels, and $100,000 spent at gentlemen's clubs.

The judge ordered Muchimbato to pay $651,068.35 in restitution to victims and to forfeit his ill-gotten gains of $1,273,403.36. Muchimba also will be subject to deportation. (Source)

General Manager Admits Embezzling $878,000 From Her Employer / Used Funds To Pay Credit Card Bills - September 2, 2025

Kristina Higgins is the former general manager of a Missouri company.

Higgins admitted issuing company checks to pay a total of $878,711 in personal credit card bills and using a stamp to add the company owner's signature on the checks. In December of 2022, she falsified information to ensure that the checks would be honored when the company enrolled in the bank's positive pay system. (Source)

County Director Of Finance Sentenced To Prison For Stealing $125,000+ In Public Funds / Used Funds To Live Lavish Lifestyle - September 2, 2025

Regene Newman exploited positions of public trust over a period of more than seven years, stealing over $125,000 intended for community programs and nonprofit organizations. She used the funds to support a lavish lifestyle, making large purchases at retailers including Sephora, Ulta Beauty, Bath & Body Works, Bra Goddess, Hobby Lobby, Target, and Macy's.

From 2015 to June 2021, Newman served as Director of Finance for the Vanderburgh County Prosecutor's Office, where she had authorized access to both an office credit card and a debit card for My Goals, a nonprofit operating under the Prosecutor's Office to assist at-risk youth.

Between March 2016 and March 2021, Newman made approximately $60,028.66 in unauthorized purchases with the My Goals debit card. To conceal the theft, she arranged for the Prosecutor's Office to make sham "donations" to the nonprofit by submitting false Accounts Payable Vouchers. These fake donations created the appearance that the funds would be used to support My Goals' mission of helping the community. During that time, Newman also made $26,381.04 in unauthorized purchases using the Prosecutor's Office credit card.

In June 2021, Newman left the Prosecutor's Office and became Business Director for Vanderburgh County Community Corrections. There, she gained access to a separate county credit card and later requested responsibility for managing the checking account of a local nonprofit that supports individuals battling addiction. Once granted access, she made an additional $10,725 in unauthorized credit card purchases and $23,929.46 in unauthorized debit card purchases. (Source)

U.S. Postal Inspector Charged With Stealing $330,000+ In Cash From Elderly Victims / Used Fund For Home Improvements, Travel & Escorts - August 29, 2025

Scott Kelley is a former U.S. Postal Inspector. He was arrested and charged for allegedly stealing over $330,000 in cash from packages mailed by elderly victims and then laundering the cash. Kelly used the stolen cash to pay for a pool patio and lighting, granite countertop for his outdoor bar, Caribbean cruise expenses and escorts. He also is alleged to have stolen cash from an evidence locker and then blamed a direct report for the missing cash.

Kelley was a Postal Inspector at the Boston Division headquarters of the U.S. Postal Inspection Service, the law enforcement arm of the Postal Service. From 2015 until June 2022, he was the Team Leader of the Mail Fraud Unit, which, among other things, investigated lottery and other scams that targeted senior citizens and other vulnerable populations. In June 2022, Kelley was transferred to serve as the Team Leader of the Mail Theft Unit, a position he held until August 2023.

Between January 2019 and Aug. 11, 2023, Kelley used deceptive emails to cause unwitting postal employees to intercept packages that a USPIS algorithm had flagged as scam, and send them to him. In total, Kelley allegedly requested that approximately 1,950 packages be intercepted and mailed to him. It is alleged that Kelley opened intercepted parcels that looked or felt like they might contain cash, and that he stole any cash inside.

7 victims who were scammed into mailing cash in parcels that Kelley allegedly intercepted, and that he opened the parcels and stole the cash. The average age of the victims was 75, with the oldest victim being 82. The victims mailed between $1,400 and $19,100 cash. It is alleged that Kelley met with one victim in person and told them that that he did not know what had happened with their package and that their loss was their own fault because they had mailed cash. None of the victims recovered their packages or their cash. (Source)

U.S. Forest Service Law Enforcement Officer Sentenced To Probation For $13,000+ Of Time & Attendance Fraud - August 27, 2025

Nathan Snead documented his regular and overtime hours on his Time and Attendance Record for each pay period and signed a certification they were correct.

On May 2, 2023, based on information Snead was not working his claimed hours, agents installed a GPS tracker on his government-issued patrol vehicle to monitor his movements. The tracker data showed Snead's patrol vehicle was stationary at his house during hours he claimed to be working.

On several occasions, Snead certified on his Time and Attendance Record he worked an 8-hour regular shift. However, his patrol vehicle remained stationary at his house for the entire 8 hours. Additionally, Snead claimed overtime hours when his patrol vehicle was stationary at his house for much of his regular shift and for the entire period of claimed overtime.

Agents also evaluated Snead's law enforcement statistics from 2021 through 2023. His productivity levels, measured via incident reports and the issuance of violation notices, were much lower than other similarly situated LEOs.

Snead was ordered to pay restitution in the amount of $13,923.77. (Source)

Law Firm Business Manager Sentenced To Prison For Embezzling $612,000 By Requesting Reimbursements For Fictitious Business Expenses - August 27, 2025

Jeremy Ubben admitted that he embezzled $612,000 from his law firm employer between March 2023 and Aug. 2024.

Ubben was employed as the firm's business manager and had full administrator rights to the firm's online payroll processing program. Beginning in March 2023, Ubben submitted and approved for himself reimbursement requests for fictious business expense expenditures totaling tens of thousands of dollars. Ubben also admitted that he laundered proceeds from his theft through his TD Ameritrade brokerage account.
(Source)

Washington University School Of Medicine Assistant Professor Admits To Embezzling $412,000 By Stealing & Selling The Schools IT Equipment - August 27, 2025

Gary Grajales-Reyes submitted false requisition requests to Washington University (WU) School of Medicine for internal and external hard drives and graphics cards falsely claiming that the computer equipment was for his WU Medicine research laboratory.

Relying upon the false requisition requests, WU Medicine purchased the requested computer equipment from its vendor, which then shipped the computer equipment directly to Grajales-Reyes' research laboratory. WashU Medicine then paid for the computer equipment.

After Grajales-Reyes received the falsely obtained computer equipment he sold the equipment by two different methods, without the knowledge or authority of WU Medicine. He sold some of the computer equipment through his personal eBay site, and he also sold some of the computer equipment to an Amazon based third-party seller.

He used the money obtained by selling the computer equipment for his own personal expenses unrelated to the work and operations of WU Medicine, and without the knowledge or authority of WashU Medicine. Over the period of his scheme, Grajales-Reyes submitted 73 false requisition requests to WU Medicine for internal and external hard drives and graphics cards, which included approximately 761 different computer parts. , WashU Medicine and Washington University paid approximately $412,163 for the computer parts, which Grajales-Reyes then sold for money which he used for his own personal expenses, unrelated to the work and operations of WU Medicine. Federal law enforcement seized a substantial quantity of collectible trading cards from Grajales-Reyes' laboratory. He had purchased the cards with some of the funds he obtained from selling the computer parts. (Source)

Company Executive Director Pleads Guilty To Embezzling $1.5 Million from Employer / Used Funds For Travel, Gambling, Etc. - August 27, 2025

Justin Marquardt admitted that he stole approximately $1.5 million from his employer's bank accounts and used those funds for his personal benefit.

Marquardt held the title of executive director at his company and by virtue of his position, had access to all company finances and financial accounts from 1994 to 2023. As part of his scheme, Marquardt, without authorization, transferred funds from his employer's bank accounts to his personal accounts and wrote himself unauthorized checks from business bank accounts.

Marquardt spent most of the money on personal expenses, including travel and gambling online and at casinos. To hide his embezzlement, Marquardt omitted these unauthorized transactions from the business's QuickBooks ledger that he provided to an accountant and tax preparer. Marquardt also recorded false and fraudulent payments as business expenses in the QuickBooks records to conceal his embezzlement. (Source)

Chief Financial Officer For Staffing Firm Sentenced To Prison For Embezzling $510,000+ / Used Funds For Travel, Jewelry, Gold And Renovations To His Personal Residence - August 20, 2025

Charles Nelson misappropriated the money in 2018 and 2019 while working in the firm's Chicago office as the Chief Financial Officer.

Nelson made a series of unauthorized credit card purchases for his personal benefit, initially on meals and travel and later on jewelry, gold, and renovations of his personal residence. Nelson used the fraud proceeds to purchase many extravagant items, including Cartier and Rolex watches, a gold and diamond bracelet, and high-end appliances for his home. Nelson executed the fraud scheme by circumventing multiple corporate controls over expenditures. (Source)

Law Firm Office Manager Pleads Guilty To Embezzling $400,000+ Over 4 Year Period / Used Funds For Personal Enjoyment & Lifestyle - August 18, 2025

Todd Chapman was employed as the firm's office manager for approximately 30 years until April 2022. During this time, Chapman was authorized to write checks from the firm's bank accounts for legitimate business expenses.

From approximately 2016 through approximately 2022, Chapman personally enriched himself by writing unauthorized checks from the law firm's accounts and client trust accounts to himself. As part of his guilty plea, Chapman admitted that he carried out his scheme by using the trust he gained from his 30-year tenure with the firm to obtain complete and exclusive control of its day-to-day finances. To conceal or disguise the embezzlement, Chapman funneled money he stole from clients through the firm's operating accounts, forged signatures on checks, created false documents, made false statements under oath in civil lawsuits by former firm clients, and made false statements to federal law enforcement agents investigating the loss of client funds at the firm.

Chapman embezzled at least $409,000 from the estates of three deceased firm clients, $100,000 that one minor client was supposed to receive upon turning 18, and $15,838.84 of an initial $20,000 settlement deposit for another minor client who suffered an injury as an infant. Chapman also embezzled $13,686.21 from a $20,375 PPP loan that the firm legitimately received to provide emergency financial aid during the COVID-19 pandemic. Chapman admitted that he spent the embezzled funds for his personal enjoyment and lifestyle. (Source)

County Employee Charged With Stealing $150,000+ / Used Funds To Support His Own Company - August 14, 2025

A former employee of the Palatka Housing Authority (PHA) in Florida, an independent government organization that helps build and create affordable housing options for those in need, is being charged with funneling more than $150,000 of federal funds provided to the organization into his own company.

Thomas Hoffman, who worked at the PHA as a network administrator and payroll administrator, according to a LinkedIn profile, is accused of committing the fraud beginning at least in July 2023 and continuing through February 2025. (Source)

Employee Sentenced To Prison For Embezzling $500,000+ From 2 Companies He Worked For / Used Funds For Friends & Acquaintances - August 14, 2025

Scott Foster was sentenced to prison for embezzling a total of $501,000 from two companies he worked for.

Foster was ordered to repay $306,199 to the St. Louis County company where he worked as a mid-level executive in human resources. Foster pleaded guilty in February to one count of wire fraud and admitted manipulating the human resources systems to create an employee account for his paramour. Foster triggered wages and benefits totaling more than $273,000 to be paid to his paramour over nearly five years, until Foster was terminated in December 2022. He also used a corporate American Express card to pay for more than $33,000 in personal travel for himself, his paramour and other friends and acquaintances.

After Foster's guilty plea, the U.S. Attorney's Office was contacted by a non-profit children's hospital where Foster had been working since June 2023. After learning about the embezzlement from the St. Louis County company, they investigated and discovered Foster had fraudulently used hospital credit cards for unauthorized personal expenses and travel, the memo says. Foster, who had received a $20,000 relocation bonus to move to the area of the hospital after being hired, instead stayed in Charlotte and used the hospital credit cards to pay for airfare and lodging to commute to his job. He also used these credit cards for personal travel, and to pay for first-class air travel to St. Louis and a hotel stay. Foster's embezzlement from the hospital did not stop even after he learned he was being investigated for the embezzlement from his first employer. Foster was ordered to pay $194,855 to the hospital. (Source)

U.S. Postal Service Mail Carrier Pleads Guilty To Role In Stealing Checks - Credit Cards From Mail / Used Funds For Trips, Luxury Goods, Etc. - August 11, 2025

Mary Ann Magdamit formerly worked as a letter carrier for the United States Postal Service in Torrance, California.

She pleaded guilty to stealing checks and debit and credit cards from the mail then selling them to her accomplices for three years, using the illicitly obtained funds to take international trips and buy luxury goods, and then flaunting the cash on Instagram.

From at least 2022 until July 2025, Magdamit stole mail containing checks, personal identifying information (PII), and debit and credit cards. She then activated the stolen bank-issued cards online, used the cards to make purchases, and sold some stolen cards to her co-conspirators.

She also arranged to have her co-conspirators cash the stolen checks, usually by people using counterfeit identity documents in the name of the check's payee. Federally insured banks and credit unions were victimized in this scheme.

Law enforcement searched Magdamit's apartment in December 2024, and seized 133 stolen credit and debit cards,16 U.S. Department of Treasury checks, and a loaded, un-serialized Glock gun. Agents also discovered luxury goods purchased with cards she stole from the mail. She also used stolen cards on international trips she took to Turks and Caicos and Aruba.

Magdamit posted on Instagram her luxury purchases and vacations, and flaunted stacks of hundred-dollar bills. Magdamit has agreed to forfeit a Rolex watch and other luxury goods. (Source)

Company Bookkeeper And Husband Sentenced To Prison For $1.4 Million Embezzlement Scheme Lasting 10 Years / Used Funds For Airline Tickets, Cruises, Etc. - July 28, 2025

From 2003 until August 2021, Valerie Joseph served as a bookkeeper for a wholesale greenhouse and garden center located in Caroline County, Maryland.

Beginning in January 2011 and continuing into August 2021, the couple conspired to defraud the business.

Robin and Valerie Joseph schemed to make unauthorized charges to three credit card accounts associated with the business for personal gain. This included American Express and Capital One accounts, along with a Lowes / Synchrony financial account.

Routinely, for more than a decade, Robin and Valerie Joseph used credit cards associated with the victims' accounts to make numerous unauthorized purchases. The theft included unauthorized credit-card charges for $200,000-plus at Walmart; $53,000-plus to AT&T for personal phone bills; $30,000-plus at a Japanese steak and seafood restaurant; and $116,000-plus to PayPal. Robin and Valerie Joseph charged more than $90,000 to Easton Utilities for utility bills; $16,000 to Chesapeake College for tuition payments; $2,500 to the University of Hawaii for college expenses; and $3,800 for cosmetics.

The couple also charged more than $195,000 to the Lowes Account. Several of the unauthorized Lowes account charges were to purchase materials and supplies to renovate their previous residence in Easton, Maryland.

Additionally, Robin and Valerie Joseph paid for airline tickets, cruises, Airbnb expenses, and hundreds of retailor gift cards using the victims' account. The couple also used the victims' account to pay more than $33,000 in veterinary expenses and charged various items related to their pets, including high-end bird cages for their tropical birds. (Source)

Civil Service Director For City Charged For Stealing $124,000+ / Used Funds To Pay Off Credit Card Debt - July 24, 2025

Civil service director (Rosa Pedraza) for the city of McAllen has been charged with theft for using a stranger's bank account to pay off more than $124,000 in credit card debt.

A probable cause affidavit for her arrest said the investigation began on June 13 when a man filed a report with McAllen police after receiving a call from Texas Regional Bank about several fraudulent transactions originating from Capital One Online. "They stated they had never had a credit card with Capital One and had not authorized anyone to use their bank information".

As the investigation unfolded, the man and his wife provided police with monthly bank statements that highlighted the unauthorized statements, all of which were linked to the Capital One credit card dating from Oct. 31, 2024 to Dec. 31, 2024. The couple also learned that the fraudulent activity went back farther. The affidavit said the alleged fraud began on Feb. 16, 2022 and lasted through May 19.

In all, the money the man lost from his bank account to pay Capital One accumulated to $124,654.71. Detectives found transactions made at various locations, including Sam's Club in McAllen and at the Lucky Eagle Casino in Eagle Pass.

Investigators were able to work with loss prevention officers and other methods to determine that a black 2020 Lexus Series 300 and silver GMC Canyon were linked to the suspect. Detectives also learned Pedraza worked for the city of McAllen and obtained her driver's license photo which they were able to link to an image of the person who used the credit card at the Sam's Club, according to the affidavit. (Source)

Banker Arrested For Role In Obtaining $2.7 Million In COVID Business Relief Funds Scheme / Used Funds For Gambling, Luxury Cars, Jewelry, Etc. - July 10, 2025

A former Wells Fargo & Co. banker (Norayr Madadi) and his brother (Vazrik Madadi) have been arrested on an eight-count federal grand jury indictment alleging they schemed to fraudulently obtain more than $2.7 million in taxpayer-funded COVID-19 relief funds and federally-guaranteed small business loans, including by submitting applications using the stolen identities.

Norayr Madadi was a banker at Wells Fargo and opened fraudulent accounts in the names of shell companies and persons including using stolen and fictious identities.

From March 2020 through April 2021, the defendants obtained millions in Paycheck Protection Program and Economic Injury Disaster Loan Program loans by submitting loan applications with false statements about revenues, operations, and employees. The defendants used fake and stolen identities to further the fraudulent scheme, including the stolen identities of two victims who are developmentally disabled and live in long-term care facilities.

The Small Business Administration (SBA) and PPP participating lenders disbursed the loans into bank accounts controlled by the defendants, including the Wells Fargo bank accounts opened by Norayr Madadi. The Madadi brothers allegedly spent the loan proceeds at casinos, paying for luxury cars and jewelry, and cash withdrawals. (Source)

Company Personnel Director Sentenced To Prison For Embezzling $500,000+ / Used Funds To Pay Debts, Vacations, Gambling Etc. - July 7, 2025

Between October 2020 and March 2022, Zachary Rugen was employed as the personnel director for a small company in St. Petersburg, Florida.

Rugen exploited that role to embezzle at least $503,372.01 from the company. He used his access to the employer's payment processing system to direct funds intended for vendors and contractors to bank accounts he controlled. Rugen also paid some of his outstanding debts with company funds. To cover the fraud scheme, Rugen electronically submitted falsified and fraudulent payment invoices. Rugen used the ill-gotten funds to live lavishly, including taking expensive vacations and gambling, and for his personal expenses. During the sentencing hearing, the victim-company's chief operating officer testified that the fraud caused substantial financial hardship from which it will take the company at least five years to recover. As a result of the embezzlement, one of the company's vendors nearly went out of business. (Source)

Company Bookkeeper Sentenced To Prison For Embezzling $300,000 From Employer For 7+ Years / Used Funds For Cruises, Vacations, College Tuition Fees, Etc. - July 2, 2025

Kayellen Inskip admitted to using the credit card issued by her employer, Mears Floral, to make unauthorized personal purchases.

Inskip pled guilty to the unlawful use of a credit card between August 31, 2021, through August 25, 2022. However, Inskip was sentenced under facts that were presented to the Court in which her true scope of her embezzlement occurred beginning in 2014 and continuing into 2022, only stopping after her fraud was discovered by company officials.

Inskip used the company card to pay for travel including airplane tickets, vacations that included cruises with Carnival Cruise Line, and vacations to Disney World, as well as entertainment, restaurants, clothing, utilities, medical bills, and she even paid college tuition and fees for her own daughter. Inskip used her position as a bookkeeper and Operations Manager with the business to authorize payments for her fraudulent purchases. Inskip would then provide false financial reports to officers in the company that allowed her to both hide her embezzlement from more than 7 years and ultimately steal nearly $300,000. (Source)

Credit Union Branch Manager Sentenced To Prison For Embezzling $330,000+ / Used Funds For Personal Gain - July 1, 2025

An auditor with Doches Credit Union In Texas, requested a sample of loans from the Hemphill branch for review. The review showed missing paperwork and unusual transactions on loans that were approved by Haley Maxine Snodgrass. Snodgrass had been employed by the Doches Credit Union since 2016, first as a teller and then as a branch manager.

An investigation conducted by a third party revealed that Snodgrass used a variety of schemes to take money from the credit union for personal gain. This included creating fraudulent loans, refinancing legitimate loans without the consent of the credit union member, misappropriating loan payments, and conducting unauthorized transactions on member accounts.

As part of her plea, Snodgrass admitted that she embezzled and willfully misapplied approximately $281,097.97 in money, funds, and assets belonging to Doches Credit Union with the intent to defraud the credit union. She also admitted that the amount of restitution owed was $330,351.39. (Source)

Union President Pleads Guilty To Embezzling $10,000+ / Use Funds For Bars, Restaurants, Etc. - June 26, 2025

Kyle Chasse, 38, embezzled over $10,000 in union funds between 2020 and 2022, while serving as the union's president.

Chasse withdrew cash and made debit purchases using the union's bank account, all without authorization by the union. The debit transactions included purchases from bars, restaurants, vending machines, and other businesses. Chasse made false statements to cover up his fraudulent use of the funds. These false statements included a union financial disclosure form filed with the federal government, in which Chasse misrepresented the amount of money he had received from the union. (Source)

County Treasurer Sentenced To Prison For Stealing $38 Million+ in County Funds By Wiring Funds To Fake Companies / Used Funds To Purchase Real Estate, Etc. - June 24, 2025

Elizabeth Gutfahr, who served as Santa Cruz County Treasurer from 2012 through 2024, embezzled and laundered approximately $38.7 million by wiring public funds from Santa Cruz County's account to accounts in the names of fake companies she had created that performed no legitimate business. Gutfahr then used the money to purchase real estate, to renovate her family ranch, to pay expenses for her cattle business, and to buy at least 20 vehicles.

Gutfahr's 10-year scheme involved approximately 187 wire transfers, which she was able to complete by undermining the two-step approval process required for transfers. Gutfahr used the token of a subordinate Santa Cruz County employee so that she could both initiate and approve the wire transfers. To cover up the scheme, Gutfahr falsified accounting records, cash reconciliation records, and reports of the County's investment accounts, thereby hiding the millions of dollars that she had stolen from Santa Cruz County. (Source)

Office Manager / Bookkeeper For Realtor Sentenced To Prison For Embezzling $453,000+ Over 5 Years / Used Funds To Pay Her Credit Card - June 18, 2025

Lauren Eldridge was an office manager and bookkeeper for nine years with Keller Williams Realty River Cities (KW) on Georgia.

KW representatives noticed some discrepancies in a KW account in Oct. 2022 and that Eldridge had moved money out of that account to other accounts. When Eldridge was initially questioned about the transfer, she did not provide a clear explanation. Eldridge resigned from her position soon afterward.

Law enforcement was notified in Jan. 2023; a review of the KW accounts revealed that a total of $453,876.68 in monthly electronic payments were made to Eldridge's personal American Express account from KW accounts between Jan. 2017 and Sept. 2022. Eldridge admitted to KW representatives and their legal counsel in Dec. 2022 that she embezzled the money from KW to pay her personal American Express credit card balance every month. She reported that she intended to pay this money back when she first began taking funds after she had charged $30,000 to her American Express for home repairs.

Eldridge was ordered to pay $453,876.64 in restitution to KW. (Source)

Finance Director For Non-Profit Organization Sentenced To Prison For Embezzling $320,000 / Used Funds To Pay For Travel For Himself, Family & Friends - June 17, 2025

Jarrett Lewis was employed by the non-profit organization (NPO) between June 2021 and October 2022.

While serving as Director of Finance, Lewis perpetrated a scheme to defraud his employer. Lewis was one of three employees at the NPO with access to the non-profit's bank account. It was part of Lewis's duties to pay bills on behalf of the organization. Lewis was also provided with a VISA card for an account belonging to the NPO and was authorized to use the VISA card to incur expenses on behalf of the NPO for goods and services related to its operations.

On 32 occasions, Lewis took advantage of his position by accessing the NPO's account and causing funds to be transferred to his personal account and for his own personal benefit. Lewis also used the non-profit's VISA to book and pay for personal travel for himself, his family, and friends.

Lewis was ordered to pay restitution of $318,000. (Source)

City Employee Sentenced To Prison For Embezzling $430,000+ / Used Funds For Entertainment Gambling, Etc. - June 17, 2025

Leo Pellegrini is the former Director of Health and Human Services and Director of the Department of Environmental Services for the City of Hoboken in New Jersey.

Pellegrini embezzled money from the City of Hoboken by diverting approximately $223,500 in payments intended for the City of Hoboken to bank accounts he controlled. Pellegrini also embezzled money from the City of Hoboken by submitting approximately $234,432.60 in his personal expenses, which the City of Hoboken unknowingly paid.

Pellegrini used the embezzled funds on personal expenses including meals, entertainment, and gambling, allowing him to live far beyond his means. (Source)

Office Manager Sentenced To Prison For Embezzling $400,000+ Over 4 Years / Used Funds For Personal Expenses - June 13, 2025

Between December 2019 and February 2023, Nichole Lawrence was employed as an office manager for a business in Western Kentucky. She used her position to embezzle approximately $400,000 from the business. Lawrence used the stolen money to pay personal expenses.

Lawrence was also ordered to pay $400,000 in restitution. (Source)

Chief Financial Officer Pleads Guilty To Stealing $211,000+ / Used Funds To Pay For Spouse's Long Term Care, Etc. - , June 6, 2025

Pamela Kahut is the former Chief Financial Officer of Pacific States Marine Fisheries Commission (PSMFC). pleaded guilty Thursday for stealing money from PSMFC's health benefit trust account.

Kahut had access to and controlled PSMFC's health benefit trust account that was created to pay benefits, fees, and other charges for PSFMC employees covered under its self-funded health care benefit program.

On September 21, 2020, Kahut wrote a check in the amount of $2,812.85 from the health benefit trust account to pay for her spouse's participation in PSFMC's long-term care insurance program.

In total, between October 2014 and September 2020, Kahut stole approximately $211,083 from PSMFC's health benefit trust account. Kahut used the funds to pay for her spouse's long-term care annual premiums, pay off her pension loans, and to pay her credit card bills. (Source)

Company Senior Staff Accountant Sentenced To Prison For Embezzling $440,000+ Using Fraudulent Invoices / Used Funds For Personal & Family Members Expenses - June 6, 2025

Between April 2022, and June 2024, Erin Martin defrauded a business, located in Amherst, NY, which employed her as a Senior Staff Accountant.

Martin reported to the Chief Financial Officer and was responsible for, among other things, ensuring that the companys vendor invoices were paid timely.

Martin created fraudulent vendor invoices addressed to her employer.

Martin would then make unauthorized electronic funds transfers from the companys bank account directly into her personal bank account, purportedly as payments on the fraudulent invoices she had created. In total, Martin caused 95 electronic funds transfers totaling $440,395.00. Martin used these funds to pay her own personal and family members expenses. (Source)

Hospital Employee Fired For Accessing 2,000+ Patients Records For 5 Years / Used Information To Promote His Healthcare Business - June 6, 2025

More than 2,000 patients at Jackson Health System in Miami, Florida, had their personal data, including names, address and medical information, accessed in a lengthy breach that spanned nearly five years. Social Security numbers weren't compromised, according to the hospital.

The data breach was conducted by a Jackson employee who accessed the information to promote a personal healthcare business.

News of the breach comes just days after an executive with the hospital system's fundraising arm was arrested on allegations that she pocketed more than $1 million through an almost decade-long kickback scheme.

This isn't the first time patient records have been breached at Jackson. The U.S. Department of Health and Human Services in 2019 fined the hospital system $2.15 million "over three patient health information breaches, including missing boxes of paper records, an employee leaking information about an NFL player to an ESPN reporter, and another employee stealing and selling other records," as the Miami Herald has previously reported. (Source)

Los Angeles County Employees Retirement Association Chief Security Officer Charged For Sending $20,000 Of County Business To His Own Business - June 4, 2025

A 42-year-old former interim Chief Security Officer for the Los Angeles County Employees Retirement Association (LACERA) has been charged with pocketing nearly $20,000 via a company he created while on the job and failing to disclose the conflict of interest

Carmelo Marquez initially worked as an independent contractor doing information security work for LACERA. In February 2023, he was named LACERA's interim Chief Security Officer. He is accused of failing to disclose to his employer that he had launched a business that sold software products and provided technical support directly to LACERA.

Marquez allegedly used his position to illegally funnel public contracts worth roughly $120,000 through his own firm and profited $19,904 through those transactions. He no longer works for LACERA. (Source)

Employee Arrested For Embezzling $330,000+ / Used Funds To Support His Family & Way Of Life - June 4, 2025

A former Lipscomb Powersports employee was arrested after alleged embezzlement from the Wichita Falls business.

Eric Skipper was charged with theft of more than $300,000 in April 2025 and according to his arrest affidavit. Lipscomb Power Sports had filed a report of the crime in July 2024 after he was fired.

Skipper's embezzlement efforts included fraudulent returns, sales records manipulating, and exploitating software loopholes. Records claimed that Skipper was one of the only person with the access to the records system, and the ability to manage cash intake and deposit returns.

Skipper admitted to the embezzlement and told investigators he took the funds to support his family and way of life. Skipper stole at total of $331,983.20 from Lipscomb Powersports. (Source)

Chemical Manufacturing Company Managing Partner Sentenced To Prison Using $250,000 Of Company Funds To Build House - May 30, 2025

Jerry Noles was the managing partner of Coil Chem LLC, a chemical manufacturing company based in Washington, Oklahoma.

Noles opened a $690,000 revolving line of credit through First National Bank (FNB) for the bank-authorized purpose of funding Coil Chem's operating expenses. Noles later caused the advance of $250,000 from the company's credit line into another account under Noles' control, then directed a coconspirator to immediately withdraw and deposit the funds into the account of a local home builder to help pay for the construction of a new home for Noles. Noles then sought and obtained a $1,200,000 home construction loan from FNB, despite the fact he had already paid a portion of the home's construction costs with the money fraudulently obtained from Coil Chem's credit line. (Source)

U.S. Government Employees Spent $40 BILLION+ Using Government Charge Cards, Some At Casinos, Bars & Nightclubs - May 19, 2025

House Oversight Chairman James Comer, R-Ky., and Sen. Joni Ernst, R-Iowa., are demanding sweeping reforms to the federal government's use of charge cards after thousands of highly questionable charges were uncovered at the Department of Defense, including at casinos, bars and nightclubs using taxpayer dollars.

In a letter addressed to Comptroller General Gene Dodaro, Ernst and Comer called on the Government Accountability Office (GAO) to launch a comprehensive review of all federal charge card programs.

The demand follows alarming findings from recent audits that point to systemic failures in oversight, including the issuance of nearly two charge cards per federal employee and more than $40 billion in spending last fiscal year alone.

The Pentagon's inspector general found nearly 8,000 Defense Department credit card transactions at "high-risk locations" – including casino ATMs – over the past year. An additional 3,246 transactions occurred at bars and nightclubs, many of them on federal holidays, Super Bowl Sunday, St. Patrick's Day, the day of UFC 300, Cinco de Mayo and New Year's Eve.

The DOD is not alone. Recent GAO reports have found agencies consistently fail to use tools to analyze purchase card data and prevent fraud, the letter notes.

The letter also highlighted the illegal practice of "split purchases," where government employees intentionally divide large transactions to stay under the $3,500 micro-purchase threshold – the largest purchase that can be put on a federal charge card. Despite being a clear violation of federal regulations, these practices reportedly continue due to inadequate monitoring and enforcement. (Source)

U.S. Postal Service Employee Arrested For Stealing $19,000+ Of Money Orders / Used Funds Personal Expenses & Gambling - May 23, 2025

Bethany LeBlanc served as the Postmaster of the Seekonk Post Office in Massachusetts from November 2023 to about February 2025. Prior to holding this position, she worked for the United States Postal Service in a variety of roles including carrier, window clerk and customer service manager.

As Postmaster of the Seekonk Post Office, LeBlanc had the authority to issue and approve "no fee" money orders. Money orders are generated by the USPS and serve as a safe alternative to sending cash or a check through the mail. "No fee" money orders are issued solely for the purpose of paying USPS-related expenses and, thus, no fee is charged.

LeBlanc generated a total of 25 no fee money orders to herself, totaling approximately $19,917. To avoid detection, LeBlanc allegedly presented false invoices for USPS expenses to clerks at the Seekonk Post Office, who would then issue the money orders for LeBlanc. It is further alleged that LeBlanc entered false information on the money orders. For two money orders, she allegedly entered "Fire Dept. Box" in the memo section to give the appearance that these money orders were used to pay for Post Office related expenses. For many money orders, LeBlanc entered the names of her relatives and associates to make it appear as if the funds were coming from sources other than the USPS. LeBlanc is accused of allegedly using the stolen proceeds for personal expenses, including thousands of dollars spent at casinos. (Source)

Law Firm Chief Financial Officer Sentenced To Prison For Stealing $1.3 Million+ Over 5 Years From San Francisco Law Firms / Used Funds For 3 Houses He Owned - May21, 2025

Tony Perkins was hired in 2017 by a San Francisco law firm and eventually became the Chief Financial Officer (CFO) of that firm as well as a related law firm.

Perkins was in a position of trust and had access to the law firms' payroll systems and end-to-end payments automation platforms. Perkins used his position to embezzle more than $1 million while he worked at the firms. From 2017 through 2023, Perkins stole more than $1.3 million and used that money for, among other things, improvements to and mortgages on three houses he owned. (Source)

Health Foundation Executive Charged With Pocketing $1 Million+ In Kickbacks For $3.6 Million Fraudulent Invoice Scheme / Used Funds To Buy Designer Handbags & Golf Cart - May 21, 2025

Charmaine Gatlin, 52, served as the COO of the Jackson Health Foundation from 2014 through 2024. The Foundation is the fundraising arm of Jackson Health System (Jackson), a nonprofit hospital and medical system that serves Miami-Dade County. In addition to philanthropic contributions, Jackson's funding comes from sales taxes, federal government programs, and other sources. As COO, Gatlin received a base salary ranging from $185,000 to $290,000. She signed a conflict-of-interest form with the Foundation preventing her from making decisions that resulted in personal gain.

The indictment alleges that Gatlin submitted false invoices to the Foundation for at least $3.6 million in goods and services that: (a) funded kickbacks to Gatlin; (b) were never provided to the Foundation or Jackson; (c) were provided to Gatlin or her relatives instead of the Foundation or Jackson; or (d) were provided to an Atlanta-based civic organization (Civic Organization 1).

Gatlin approved approximately $2 million in invoices to a Georgia-based audiovisual company for services that were not provided to the Foundation. Instead, the vendor allegedly paid $1 million in kickbacks directly to Gatlin, some of which she used to pay her personal credit card bill. The indictment alleges that Gatlin coached the vendor, via email, on how to falsify invoices.

The indictment also alleges that Gatlin falsified invoices from a merchandise vendor who, at Gatlin's request, bought her expensive designer gifts from Louis Vuitton, Gucci, and Apple. Gatlin also submitted a false invoice to the Foundation to cover the purchase of a new rose gold-colored golf cart that she had delivered to her Weston, Florida home in September 2023. (Source)

Meatpacking Plant Worker Convicted For Role In $2.4 Million COVID Pandemic Benefits Fraud & Money Laundering Conspiracy / Used Funds To Buy A Tractor Trailer - May 9, 2025

Yovany Ciero, 48, was convicted of three counts of wire fraud, 23 counts of money laundering, one count of engaging in a monetary transaction in property derived from a specified unlawful activity, and one count of money laundering conspiracy.

The evidence at trial showed that Ciero is a former Sergeant in the Cuban military who crossed the Mexican border nearly twenty years ago after his request for a visa to enter the United States was denied. In 2020, Ciero was working at an Algona meatpacking plant when the COVID-19 pandemic began. Beginning in July 2020, Ciero, and over one hundred other immigrants from Cuba, obtained fraudulent Paycheck Protection Program (PPP) loans on the false and fraudulent pretenses that they were self-employed businesspeople who earned approximately $100,000 in gross income in 2019 when they actually worked at the meatpacking plant or elsewhere in 2019.

Ciero was one of six "bundlers" in the fraudulent PPP loan scheme.

Ciero's role was to recruit individuals into the scheme, obtain their personal identifying information for the fraudulent loan applications, and then pass that information to others who submitted the fraudulent loan applications to lenders who were participating in the PPP. The evidence established that over $4 million in fraudulent loan PPP applications were submitted, and the government lost over $2.4 million as a result.

Once the individuals received their fraudulent PPP loan funds, typically $20,000 each, Ciero served as a "funnel" in a money laundering conspiracy. Ciero collected fees that the organizers of the scheme charged the applicants, typically $3,000 per $20,000 fraudulent loan.

Ciero also obtained two fraudulent PPP loans for himself and his paramour. Ciero used most of this PPP loan money to purchase a semi-truck. Ciero is the sixth former Iowa meatpacking plant worker convicted in the PPP scheme. (Source)

Credit Union Employee Sentenced To Prison For Embezzling $65,000+ / Used Funds Spending Sprees - May 8, 2025

Throughout 2023, Kelly Jo Muzzana served as the Operations Manager for Altana Federal Credit Union in Billings, Montana. In that role, Muzzana had access to customer data and was responsible for managing Altana's entire fraud-alert process. This included supervising the employees who documented customers' fraud claims and facilitating what funds were reimbursed by Altana. Muzzana also managed the fraud reporting system and was entrusted to independently authorize bank cards that were re-issued to customers or returned to the bank through the mail.

During her time as Operations Manager, Muzzana created duplicate bank cards for customers' accounts and took them home with her. She did the same with cards that Altana received in the mail that were undelivered to customers. Muzzana took numerous bank cards from Altana and used them to make purchases online and in retail stores around Billings, Montana such as Target and Walmart.

After using their cards to finance her private spending, Muzzana personally handled many of the subsequent fraud claims to prevent detection by law enforcement.

Eventually, an Altana customer reported one of Muzzana's fraudulent purchases to law enforcement. When a detective called Altana to investigate, Muzzana downloaded a recording of the call and, upon learning of the investigation, fled the building and never returned. (Source)

Property Manager Plead Guilty To Stealing $1.6 Million+ Over 5 Years / Used Funds For Personal Use - May 5, 2025

In January 2017, Sherrie Billings worked as a regional property manager for Manhattan Management Company, LLC (MMC), out of New York. MMC owned four apartment complexes in Oklahoma City. Her duties included maintaining daily upkeep, maintenance, and inspections of the properties, and she had access to an MMC bank account and credit card for such maintenance.

From January 2017 through July 2022, Billings defrauded MMC by issuing unauthorized checks from MMC's bank account and utilizing the company credit card, both for her own personal use. During this time period, Billings issued approximately 385 unauthorized checks, illegally withdrawing approximately $1,660,238.00 from MMC's account. To conceal her scheme, Billings manufactured fraudulent payment vouchers to legitimate vendors and emailed the fraudulent vouchers to MMC's bookkeeper to be added to the company ledger. Billings also used the MMC credit card for personal expenses, which defrauded the company out of approximately $49,798.00. (Source)

Information Technology Manager Pleads Guilty To Using 3 Different Fraud Schemes To Steal $1Million From Employer / Used Funds To Purchase Personal Electronic Devices - May 2, 2025

Laguna Welch worked for the company from 2011 to 2024. He was promoted to Information Technology Manager in 2018.

As early as 2017, Welch used the company's Amazon business account to make unauthorized personal purchases from Amazon.com. Between 2017 and 2023, those purchases totaled at least $43,000. Welch primarily purchased electronics such at televisions, laptops and more—all for personal use. In 2019, Welch began using his company credit card for personal purchases through other online retailers such as Apple, Alaska Airlines, Instacart, and BestBuy. Between 2019 and 2024, those unauthorized personal purchases totaled at least an additional $60,000.

The scheme really accelerated in January 2021 when Welch began making payments to himself disguised as payments to a computer services company. Welch created a series of email addresses and payment processor accounts using a business name that was very similar to a legitimate computer services company based in Washington State. Welch then used Algas-SDI company credit cards to pay the computer services company under the guise that the company was providing IT equipment and services to Algas-SDI. However, the legitimate computer services company had no relationship with Welch and never provided any services or equipment to Algas-SDI. The credit card payments Welch made from Algas-SDI's credit cards went directly to the payment processor accounts that Welch controlled. Between 2021 and 2024 Welch used this scheme to transfer approximately $879,175 from company accounts to his own accounts.

In all, between 2017 and January 2024 Welch secretly made at least 250 fraudulent charges for the third-party vendor he controlled. He made at least 140 unauthorized purchases with retailers using the company credit card and at least 100 fraudulent purchases on the company's Amazon account.

While Welch profited some $950,000 from his theft, the loss to ALGAS-SDI was approximately $982,520 due to various fees on the transactions. (Source)

City Police Chief / City's Administrator Is Accused Of Stealing $313,000 From City To Support His Personal Business - May 1, 2025

Daniel Paulino is the former Police Chief and City Administrator of Velda City, Missouri.

Paulino is accused of fraudulently obtaining $313,420 in city funds through a series of fraudulent transactions.

Paulino used the city's credit card to make about 828 charges for his personal expenses totaling about $145,428. Paulino used the city credit card on about 17 additional occasions to transfer Velda City funds totaling about $43,870 to a business he owned, R & B Towing, and one owned by his spouse, Renovations-STL. The city funds were ultimately transferred to either Paulino's personal bank account or the account for another company he owned, D and H Towing.

Paulino caused about eight city checks to be issued in a total amount of about $34,374 to pay third party vendors for his personal expenses, the indictment says. One $25,500 city check was used to pay for a 2007 International tow truck that was then registered in Paulino's name and used by Paulino's privately-owned towing company, the indictment says. Paulino caused Automated Clearing House (ACH) transactions to be made from a city account to pay third party vendors for $2,575 in personal expenses, the indictment says.

Paulino also caused about 20 direct deposits totaling $30,667 in city funds, purportedly for additional payroll, into his personal account, the indictment says.

He caused about 55 direct deposits of a total of about $54,693 in Velda City funds, purportedly for his spouse's payroll, to be sent to his personal bank account, the indictment says. Paulino's spouse was being paid for work that was not actually performed in the city's public works division during the years 2021 through 2023 and Paulino used that money for his own personal expenses, the indictment says.

Paulino caused three city checks totaling $1,800 to be fraudulently issued to him. Paulino transferred about $58,171 from his personal or business bank accounts to Velda City's bank account or the city's credit card to conceal his crimes.

Paulino used the money for travel, automobiles, pool supplies, utilities at his personal residence and food and beverage charges, the indictment says. (Source)

City Finance Director Sentenced To Prison For Embezzling $950,000 / Used Funds For Personal Expenses - April 30, 2025

Robert Burgett worked for the City of Homewood in Alabama, as its Finance Director.

Between at least May 2023 and about March 2024, Burgett used that position to embezzle almost $950,000 from City of Homewood bank accounts.

Burgett concealed his conduct by first moving the City's funds into a commercial bank account he controlled before transferring the funds into his personal account. Burgett also altered City bank account statements and made false journal entries in City accounting records. Burgett ultimately used the embezzled funds for personal purposes. (Source)

Medical Practice Chief Operating Officer Sentenced To Prison For Stealing $692,000+ / Used Funds For Travel, Home Improvements, Etc. - April 29, 2025

Francisco Ortiz, 50, is the former Chief Operating Officer of a Morgantown, West Virginia medical practice.

Ortiz defrauded Wedgewood Physicians, Inc. by diverting more than $650,000 for his own benefit. Ortiz used the funds to pay for personal items such as travel, home improvements, and online purchases. Ortiz also diverted some of the money for the benefit of co-defendant, James Mersing, a physician formerly employed by the practice. Mersing pled guilty to his role and was sentenced in October 2024.

Ortiz was ordered to pay restitution in the amount of $692,176.19. (Source)

Business Manager For School District Sentenced To Prison For Stealing $340,000 / Used Funds For Trips To Walt Disney World - April 25, 2025

Brandon Looney stole nearly $340,000 from Trinidad ndependent School District (ISD) in Texas, between 2017 and 2023 while he served as Trinidad ISD's business manager. Federal law makes it a crime for someone to steal from an organization receiving more than $10,000 in federal funds annually.

Looney used the stolen funds to purchase personal trips to Walt Disney World and on spending sprees at the Disney Store. Trinidad ISD is one of the poorest school districts in Texas and suffered adverse financial consequences as a result of Looney's theft.

Looney worked with the Financial Litigation Unit of the U.S. Attorney's Office to liquidate his available assets, including his home, to pay $200,000 of the restitution before sentencing. The remaining balance of the restitution judgment will be collectible for 20 years after the termination of Looney's incarceration. (Source)

Bank General Counsel Sentenced To Prison For Embezzling $7.4 Million Over 10 Years / Used Funds To Purchase Vacation Property, Luxury Vehicles, Etc. - April 24, 2025

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 in Connecticut.

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, Blose 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, and used the stolen funds to purchase a vacation property on Kiawah Island in South Carolina, for construction of his Connecticut home, and for luxury vehicles, jewelry, private jets charters, multiple country club memberships, and other expenses. (Source)

Employee Pleads Guilty To Embezzling $305,000+ / Used Funds To Purchase New Car - April 15, 2025
Jennifer Cabral admitted that she stole approximately $306,034.28 from her employer's bank account and used those funds for her personal benefit and use.

Cabral accessed her employer's accounting software and directed payments to her own personal bank accounts through the employer's online account at a local financial institution. Cabral used those funds for various personal benefits including vehicle payments toward the purchase of her car, which was forfeited as part of the plea agreement. (Source)

Bank Officer Pleads Guilty To Embezzling $122,000+ / Used Funds For Gambling, Paying Debit, Retail Purchases - April 10, 2025
Edward Jenkinson was employed as a bank officer at Bank 1, an FDIC insured institution that was a member bank of the Federal Home Loan Bank of Atlanta.

As a bank officer, Jenkinson was responsible for managing a Bank 1 financial center located in Tampa. One of Jenkinson's duties was to oversee the Automated Teller Machine (ATM) and teller cash drawers at the financial center.

Between March and November 2024, Jenkinson embezzled FDIC-insured funds. As part of his embezzlement scheme, Jenkinson redeemed certificates of deposit without the customers' knowledge or consent. He then prepared deposit tickets and deposited the redeemed funds in customer checking accounts. Subsequently, Jenkinson embezzled the funds from the victim customers' accounts and drafted cashiers' checks payable to himself, which he deposited into his own bank accounts. Jenkinson depleted most of the embezzled funds through cash withdrawals. He also embezzled $52,000 from the ATM machine at the Bank 1 financial center he managed in Tampa, as well as $2,500 from a bank teller drawer. Jenkinson spent the embezzled funds on gambling, paying off debt, and retail purchases. (Source)

Tech Employee Sentenced To Prison For Embezzling $550,000+ / Used Funds For Trips, Private Jets, Luxury Hotels, Etc. - March 21, 2025
The first scheme began in 2019, when Westcott Curley embezzled money from his then-employer by misusing cloud computing resources and accounts available to him as an employee. Curley used employer funds and his employee work authorizations to purchase cloud computing resources, then sell or lease 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 trips on private jets, luxury hotel stays and a penthouse apartment at Seattle's Harbor Steps complex. Even after Francis-Curley was caught and fired, he emailed customer service and corporate executives in an effort to receive an additional half-million dollars.

In 2020, Curley defrauded the Paycheck Protection Program (PPP), 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 qualified for assistance, when in fact they 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, Curley applied for and obtained a credit card in the name of his former significant other. Curley used the card for more than $1,000 in personal expenditures. (Source)

School District Employee Sentenced To Prison for Stealing $314,000+ Of Federal Funds / Used Funds For Travel, Home Improvements, Etc. - March 20, 2025

Ernesto Villarreal Jr., 43, was employed as the Business Manager and served as the Tax Collector and Assessor for the Valentine ISD, in Valentine, Texas.

Villarreal was sentenced to prison for wire fraud and theft concerning programs receiving federal funds.

During his time as an agent of Valentine ISD, Villarreal schemed to defraud Valentine ISD by using two ISD credit cards to make hundreds of unauthorized personal purchases totaling over $100,000; issued over $10,000 in unauthorized checks to himself from Valentine ISD accounts; and issued over $20,000 in unauthorized checks from Valentine ISD accounts to cover personal expenses owed to a credit card company. He also changed the bank account information for certain current and former employees, then generated over $100,000 in fraudulent payments to those current and former employees, for work that did not actually occur. Villarreal then routed those payments to his own personal bank accounts, all without the knowledge or permission of the employees.

Villarreal used the ill-gotten funds for hundreds of personal purchases, including but not limited to purchases for travel, lodging, home improvements, hardware store purchases, personal cell phone bills, fuel, oil changes, convenience store purchases, Airbnb rentals, personal flight purchases, and various other unauthorized purchases. The total loss to Valentine ISD was $314,497.74. (Source)

Office Manager Of Senior Assisted Living Facility Sentenced To Prison Embezzling $1.5 Million / Used Funds To Buy Pickup Truck & Gamble - March 20, 2025

Amy Curry worked as an office manager and bookkeeper at Silver Bluff, LLC (Silver Bluff), a senior living and care facility in Canton, North Carolina.

As part of her duties, Curry had access to and control over Silver Bluff's bank accounts and accounting records. From December 2022 to April 2023, Curry made at least 154 unauthorized bank transfers totaling over $1.5 million from the facility's bank accounts to bank accounts controlled by Curry and her then-boyfriend, J.C.

To avoid detection, Curry deleted the wire transfer history from Senior Bluff's bank accounts and altered the notification settings to prevent Silver Bluff employees and management from receiving alerts. Curry also made handwritten notes on Senior Bluff's bank statements, falsely noting that the fraudulent transfers were for payroll. Court records show that Curry used the embezzled funds to pay for personal expenses, including to purchase a pick-up truck. Curry and J.C. also spent over $700,000 of the embezzled funds gambling at casinos. Curry embezzled at least $1.5 million. (Source)

U.S Postal Worker Found Guilty Of Stealing $1.6 Million+ In Checks From U.S. Mail / Used Funds For International Travel, Etc. - March 14, 2025

Between December 2020 and March 2023, Hachikosela Muchimba was an employee of the U.S. Postal Service when he executed a scheme to steal U.S. Treasury checks and private party checks from the U.S. mail.

Muchimba then deposited the checks, which he either altered and/or falsely endorsed, into bank accounts under his control. Muchimba altered some of the checks by removing the name of the proper payee on the checks and replacing it with his own name. Bank surveillance footage captured images of him making deposits and withdrawals of the funds. The total amount of the U.S. Treasury checks fraudulently deposited into Muchimba's various bank accounts was just over $1.6 million.

Muchimba used the proceeds of the stolen checks to fund a lavish lifestyle that included international travel, stays at luxury hotels, and purchases at gentlemen's clubs. (Source)

Employee Of Online Car Sales Company Sentenced To Prison For Embezzling $2 Million / Used Funds For Lavish Lifestlye & Luxury Automobiles - March 12, 2025

Beginning in October 2018 John Whisenant worked in a variety of roles at the online used car sales company. About a year after he began with the company, Whisenant was promoted into a role where he had access to the company bank accounts and accounting software.

Beginning in about June 2019 and continuing until November 2021, Whisenant used his access to make 57 wire transfers totaling over $2 million into accounts he controlled. Whisenant disguised the transfers as legitimate business expenses in the company's accounting software with a variety of false entries. Whisenant defrauded the company of $2,084,799.

Whisenant used some of the money for a lavish lifestyle. He bought luxury automobiles such as Porches and Mercedes. He spent $123,096 for a 2022 Audi E-Tron and bought a $98,100 Tesla. He rented luxury homes in Southern California and purchased two airline tickets to Paris at a cost of nearly $23,000 each. More than $1 million went to pay his credit card debts.

The fraud on the company accounts was discovered when a bookkeeper began a more comprehensive review of the company's financials in January 2022. Whisenant resigned abruptly in February 2022.

When confronted by the FBI, Whisenant tried to blame the embezzlement on the company CEO. As prosecutors noted in their sentencing memo the impact on the company has been severe. "Whisenant's fraud seriously harmed his victims. His betrayal "traumatized" his co-workers and destabilized the company's finances.

Just before his July 2024 sentencing date, Whisenant sent an email to his pretrial services officer saying, "I'm not ready to go to jail yet." Despite his efforts to evade police, the FBI located and arrested him on August 14, 2024. (Source)

Employee Sentenced To Prison For Embezzling $440,000 From 2 Different Employers / Used Funds To Pay Credit Cards - March 11, 2025

Between September 2017 and April 2020, Jasmyne Botelho stole at least $280,000 from her employer. Specifically, Botelho directed payments purportedly intended for the company's vendors to bank accounts she controlled and used company funds to make payments on personal credit cards and an auto loan. To hide her scheme, Botelho falsified her employer's books and records to make it appear as though the payments had in fact been sent to legitimate vendors rather than to Botelho.

Between May 2022 and December 2023, Botelho improperly inflated her payroll from another employer by more than $160,000. She concealed her scheme by manipulating her employer's payroll and accounting software to hide her inflated payroll as well as phony "reimbursements" she paid herself.

Botelho was also ordered to pay restitution and forfeiture orders of $443,122.59.(Source)

Boyfriend Of A Senior Level Employee For Pharmaceutical Company Sentenced To Prison For Role In $2.3 Million Fraudulent Invoice Scheme Involving Employee / Used Funds To Purchase Mercedes-Benz, Diamond Engagement Ring, Freightliner Trucks And A $1.9 Million Condo - March 10, 2025

The boyfriend of a senior level employee at the multinational pharmaceutical company Takeda Pharmaceutical Company Limited (Takeda) was sentenced to prison for setting up a fake consulting company that billed Takeda for services it never actually provided.

Samuel Montronde was also ordered to pay $2.3 million in restitution. Montronde was arrested and charged in January 2023 along with his girlfriend Priya Bhambi a former senior employee in the technology operations group of Takeda.

In 2022, Montronde and Bhambi orchestrated and executed a scheme to defraud Takeda of at least $2.3 million in payments for purported consulting services by submitting fabricated invoices on behalf of a sham consulting company. Bhambi had previously engaged in the same fraud using a different sham consulting company, resulting in payments from Takeda totaling nearly $300,000 for consulting services that were never provided.

In February 2022, Montronde and Bhambi incorporated a sham consulting company, Evoluzione Consulting LLC (Evoluzione). Later, Bhambi created a website for Evoluzione with false information, including fabricated blog posts, to make it appear that Evoluzione was a legitimate consulting business.

After incorporating Evoluzione, Bhambi, in coordination with Montronde, submitted a statement of work to Takeda and caused Takeda to sign a master services agreement with Evoluzione and issue a purchase order to Evoluzione for consulting services with a total cost of $3.542 million. Then, between March and May of 2022, Bhambi and Montronde fabricated and submitted five separate invoices to Takeda for services that Evoluzione had not performed, each in the amount of $460,000. The defendants also created a fictional employee "Jasmine" to handle communications with Takeda. When questioned by Takeda employees, Bhambi made false representations regarding the services purportedly provided by Evoluzione. Before discovering the scheme and terminating Bhambi, Takeda, relying on these false representations, paid all five of the invoices to business accounts opened by Montronde in the name of Evoluzione.

The couple used the fraudulently obtained funds to purchase a Mercedes-Benz Model Class E, a diamond engagement ring, freightliner trucks, a $1.9-million 2-bedroom condo in Boston's Seaport District and a $50,000 wedding venue deposit. These assets are now subject to the Court's forfeiture order. (Source)

Information Technology Manager For Non-Profit Organization Sentenced To Prison For Embezzling $360,000+ / Used Funds To Build House - February 28, 2025

From April 2015 to May 2020, Kyriakos Kapiris worked as the Information Technology Manager at Venture Community Services (VCS), a non-profit organization in Sturbridge, Mass. that services developmentally disabled members of the community. As part of his responsibilities, the organization provided Kapiris access to two company credit cards to purchase equipment and services as needed.

Beginning in 2016, Kapiris used the two company credit cards to purportedly purchase equipment from two vendor accounts on the web app Square and one account on Amazon. In reality, Kapiris created the three vendor accounts to embezzle the funds and fabricated sales invoices for purportedly purchased equipment to conceal the scheme. Kapiris used the names of legitimate Massachusetts companies for the two Square accounts and created the Amazon account in the name of a company that he controlled, "NetworkingPlus."

Kapiris linked the three vendor accounts to several of his own personal accounts at Bank of America into which he transferred the fraudulent proceeds. Kapiris then used the stolen funds for personal expenses, including to build a house. The house was forfeited by the government and sold. (Source)

Company Account Manager Sentenced To Prison For Stealing $1.1 Million+ From Employer / Used Funds For Vehicles, Jewelry, Etc. - February 21, 2025

Amy Shelton began working as an account manager for her employer in 2015. She was entrusted with handling payroll, paying bills, collecting rent, and updating financial documents.

From May 2019 through November 2022, Shelton wrote more than 150 checks to herself, totaling more than 1.1 million dollars. With those funds, Shelton purchased luxury items, including recreational vehicles, purses, jewelry, and dozens of firearms. Further, Shelton did not report her income accurately and falsified her tax refunds.

Shelton was ordered to pay $870,934.67 in restitution to her former employer. (Source)

County Health Department Official In Pleads Guilty To Embezzling $260,000 / Used Funds To Pay Credit Card - February 20, 2025

Hugo Huacuz is a former employee of the Taney County Health Department in Missouri.

Huacuz embezzled approximately $260,000 from the agency between March 23, 2022, to Nov. 14, 2023.

Huacuz caused the health department to write checks to Argon Investments, LLC, a company organized by Huacuz and his wife. Huacuz forged the signatures of health department members, using their identities without their permission. Huacuz caused the health department to issue 15 checks totaling approximately $259,000, which were deposited into the bank account of Argon Investments.

Huacuz used the stolen funds for personal expenses charged to his personal credit card, including automobile insurance, maintenance, repair and parts; restaurants; home construction items; gasoline; airline tickets and travel, including to Chicago, Illinois, New York State, San Diego, California, College Station, Texas, Nashville, Tennessee, Las Vegas, Nevada, and Portland, Oregon; utilities; dry cleaning; clothing; dental and medical care; and payments to the Missouri Secretary of State's office for Argon's LLC fees.

Health board members were not aware of the existence of Argon Investments or that any checks had been issued to Argon Investments.

In order to conceal his scheme from the board, Huacuz caused these checks to be coded as payments to Sanofi Pasteur, Inc., a multinational pharmaceutical company. Huacuz falsely reported to the health department's board that some of the checks written to Argon Investments were for items purchased from Sanofi, and created false invoices from Sanofi purportedly for the purchase of pharmaceutical and medical items, including COVID-19 testing kits.

In November 2023, the director of the Taney County Health Department received information concerning Huacuz's job performance. The information stated that Huacuz was frequently absent from his job and that he had other businesses he was operating independent from his job at the health department. After reviewing the information, the director met with Huacuz on Nov. 13, 2023, and placed him on administrative leave. Huacuz went to the bank immediately afterward and withdrew more than $24,000 from the Argon bank account, leaving a balance of $100 in the account. (Source)

Bookkeeper Sentenced To Prison For Stealing $1.6 Million+ From 2 Small Businesses For 6 Years / Used Funds For Luxury Apartment Rental, Car Payments, Shopping, Vacations - February 3, 2025

From 2016 to 2022, March Weiss (Age 50) engaged in a scheme to defraud two Mooresville, N.C. small businesses that employed him as a bookkeeper.

Over the course of the scheme, Weiss, who was a trusted employee, abused his position and access to the companies' financial accounts to make more than 100 fraudulent transfers totaling $1.6 million from the companies' accounts into bank accounts under Weiss's control. Court documents show that Weiss began to embezzle from the second company while he was already stealing from the first one. To disguise the fraud, Weiss created fake entries in the victim companies' books and records, categorizing the fraudulent transfers as payments to existing vendors for software development, and advertising and marketing expenses.

Weiss used the embezzled funds, in part, to pay for his personal lifestyle, including rent payments for a luxury apartment uptown; payments for high-end vehicles, including an Audi and a Mercedes-Benz; purchases at luxury retail stores, including Luis Vuitton, Gucci, Neiman Marcus, and Tiffany, among others; and luxury vacations, including multiple stays in The Ritz Carlton hotel. (Source)

Rail Systems Assistant Chief Engineer Pleads Guilty Defrauding Company Of $8.5 Million Through False Invoicing Scheme / Used Funds For His Business - January 23, 2025

John Pigsley is the former Assistant Chief Engineer of Facilities for Keolis Commuter Services (Keolis).

Pigsley pleaded guilty to defrauding Keolis of over $8 million and to defrauding the IRS.

Keolis has operated the MBTA commuter rail system since 2014 under an annual contract of $291–$349 million. Between 2014 and November 2021, Pigsley was employed as Keolis' Assistant Chief Engineer of Facilities and was responsible for the maintenance of MBTA Commuter Rail Facilities and their engineering operations, including corrective repair and project management for assets and maintenance and ordering and approving his subordinates' orders of electrical supplies from outside vendors for Keolis. Pigsley also operated a separate construction company called Pigman Group. Rafferty was the general manager of LJ Electric, Inc., an electrical supply vendor to which Keolis paid over $17 million between 2014 through 2021.

Between July 2014 and November 2021, Pigsley and Rafferty defrauded Keolis of over $4 million through a false LJ Electric invoicing scheme. Specifically, Rafferty purchased vehicles, construction equipment, construction supplies and other items for Pigsley, Pigman Group and others, and Pigsley directed Rafferty to recover the cost of these items by submitting false and fraudulent LJ Electric invoices to Keolis.

Rafferty spent more than $3 million on items for Pigsley and others – including: at least nine trucks; construction equipment including at least seven Bobcat machines; at least $1 million in home building supplies and services; and a $54,000 camper– for which Keolis paid Rafferty more than $4 million based on false LJ Electric invoices.

In addition to the false invoicing scheme, Pigsley directed Keolis to purchase copper wire which he then stole and sold to scrap metal businesses, keeping the cash proceeds for himself. To conceal the theft, Pigsley personally picked up the copper wire orders from vendors or had the orders delivered to his Beverly home. Pigsley then personally transported the wire to scrap yards where he traded it for thousands of dollars in cash several times a month and sometimes more than once a day. Pigsley obtained more than $4.5 million in cash by stealing and scrapping the copper wire. (Source)

Banking Executive Pleads Guilty To Embezzling $4.2 Million From Customers Over 12 Years / Used Fund To Pay For Luxury Lifestyle - January 8, 2025

William Garrow was hired by the Bank of Oklahoma in August 2007 and promoted to Senior Vice President. He served as a financial advisor and provided investment and banking services to wealthy banking clients until he was terminated in March 2024.

From September 2012 through April 2024, Garrow admitted to stealing from at least 16 client accounts. Garrow fraudulently transferred funds or issued cashier checks without authorization and consent from his clients and then deposited those funds into accounts that he controlled at other financial institutions.

Garrow further admitted that his actions were wrong and that the funds were used to pay for his lifestyle. (Source)

Diversity Program Manager For Facebook & Nike Sentenced To Prison For Role In Stealing $4.9 Million+ / Used Funds To Live Luxury Lifestyle - May 13, 2024

From January 2017 to September 2021, Barbara Smiles led the Diversity, Equity, and Inclusion (DEI) programs at Facebook and was responsible for developing and executing DEI initiatives, operations, and engagement programs. In her position, Smiles had access to company credit cards. She also had the authority to submit purchase requisitions and approve invoices for authorized vendors of Facebook.

Smiles used her position at Facebook to cheat and defraud the company. She caused Facebook to pay numerous individuals for goods and services that were never provided and then directed those individuals to kick back the fraudulent proceeds to her, often in cash.

Smiles recruited numerous individuals to participate in the scheme. These individuals included friends, relatives, former interns from a prior job, nannies and babysitters, a hair stylist, and her university tutor. She also caused Facebook to make payments for her benefit to others who did not pay kickbacks. For example, Furlow-Smiles caused Facebook to pay nearly $10,000 to an artist for specialty portraits and more than $18,000 to a preschool for tuition.

As she had done at Facebook, Smiles circumvented the vendor process at Nike to commit fraud. She linked her Nike corporate card to her PayPal and Venmo accounts. She then paid her associates with PayPal and Venmo, causing fraudulent charges to her Nike card. The associates kicked back portions of the payments to Smiles, who submitted fraudulent expense reports to Nike to cover her tracks. The expense reports falsely claimed that the payments were related to the Juneteenth event.

In total, Smiles stole more than $4.9 million from Facebook and over $120,000 from Nike based on fictitious charges and fraudulent invoices. She used the money to fund a luxury lifestyle in California, Georgia, and Oregon. (Source)

And Many More……

EMPLOYEE CONTINUOUS MONITORING AND REPORTING SOLUTIONS

Employee Background Investigations Vs. Employee Continuous Evaluation & Reporting (ECMR)

Background investigations and reinvestigations are a "Point In Time" snapshot of the trustworthiness of an employee. In reality the employee is trusted at the time of the investigation.

Some companies are now beginning to use "Post-Hire" solutions that allow the employer to "Continuously" monitor an employee for Indicators of Concern. Companies can now proactively identify employee risk and preemptively address a problem before it escalates.

INTERNAL data sources are very important for Insider Threat detection.

Equally important is knowing what **EXTERNAL** data sources are also available to create the "Big Picture" of potential / actual Insider Threats.

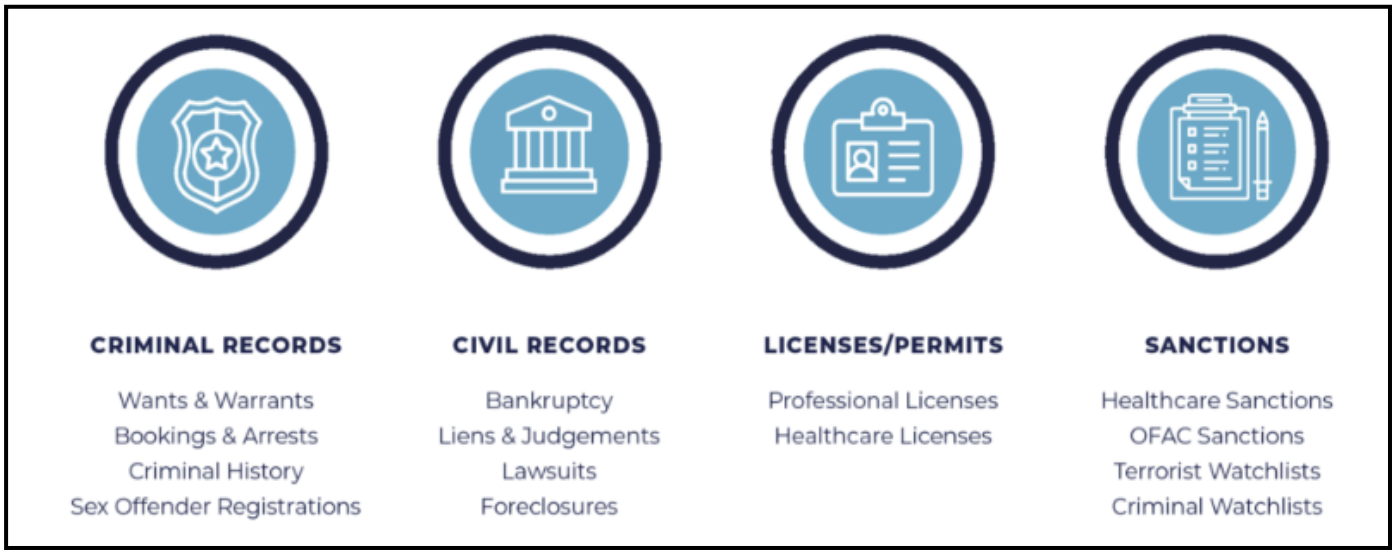
EXTERNAL data sources can provide insights into employee problems such as financial, criminal, etc. Excessive credit card utilization is another possible indicators the employee may have financial problems.

Being able to **PROACTIVELY** identify and **RESPOND** to employee risks is critical for Insider Risk Management.

ECMR solutions can pull data from over 25,000 public data sources. These records include court records, license registration, civil records, educational degrees, and public certifications.

This ECMR presentation on the link below, produced by the NITSIG provides some eye opening real life examples of what can be detected about an employee using external data sources.

https://www.nationalinsiderthreatsig.org/itrmresources/Using%20External%20Data%20Sources%20For%20Insider%20Threat%20Detection%20And%20Mitigation.pdf



Examples Of Where Implementing ECMR Might Have Prevented These Incients

Former Xerox Employee Receives Life In Prison For Credit Union Robbery / 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.

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.

Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy. (Source)

Jury Awards Over $1 Million In Negligent Hiring Lawsuit Involving Workplace Violence - November 15, 2016

A jury in Texas has awarded more than $1 million in a negligent hiring lawsuit filed against a company on behalf of an employee and war hero who was killed in 2015, while on the job, by a co-worker.

Steven Damien Young shot and killed co-worker Jacob Matthew Cadriel with a 38-caliber handgun. Young was arrested and charged with murder. He is currently serving a 45 year sentence.

In 2008, Young was "arrested, charged and convicted in Harris County of the offense of carrying an illegal weapon on the jobsite." In 2014, he was "arrested and charged in Harris County with the offense of making a terroristic threat." **He was out on bond awaiting trial when he murdered Cadriel.**

The negligent hiring lawsuit claimed that Woven Metal Products, who owned the facility where both Young and Cadriel worked, failed to "conduct comprehensive employment background checks and criminal record searches on their employees. This negligence provided an unsafe workplace for employees.

The company was negligent because it "failed listen to numerous workers at the facility who repeatedly told them about the erratic and unstable behavior of Young" and also "failed to provide any training or education on identifying and handling this type of violence behavior in the workplace." (Source)

INSIDER THREATS DEFINITION / TYPES

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

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

WHO CAN BE AN INSIDER THREAT?

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees (**1** - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (**2** - Failure By Action, Behavior Or Response) (**3** - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- ☐ Opportunist Employees (**1** - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (**2** - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (**3** - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- ☐ Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)
- ☐ Employees Involved In Foreign Nation State Sponsored Activities (Recruited - Incentives)
- ☐ Employees Ideological Causes (Promoting Or Supporting Political Movements To Engage In Activism Or Committing Acts Of Violence In The Name Of A Cause, Or Promoting Or Supporting Terrorism)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

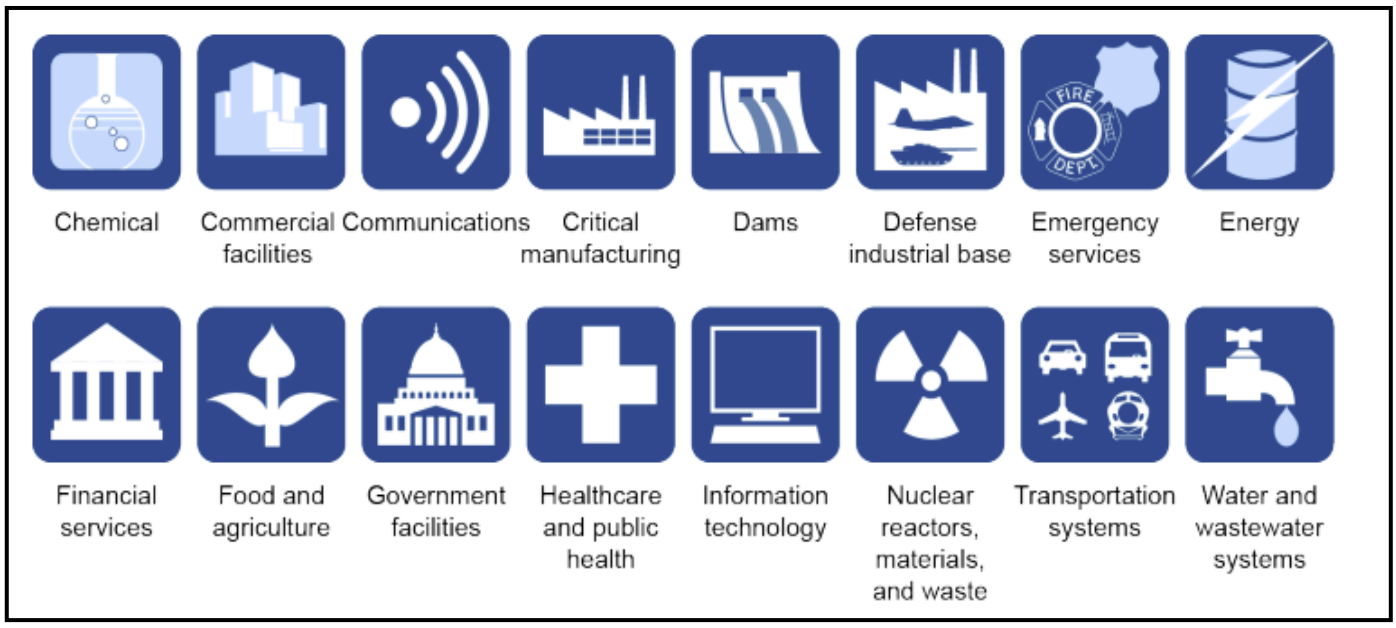
Other Damaging Impacts To An Employer From An Insider Threat Incident

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

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

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



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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

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 (IRM) Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the 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.

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE
2014 To Present / Updated Daily
The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**6,700+ Incidents**).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

The Insider Threat Defense Group (ITDG) provides organizations with the **core skills / advanced knowledge, resources and technical solutions** to identify, manage, prevent and mitigate Insider Risks - Threats.

Since 2009, the ITDG has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction. ITDG training courses and consulting services have empowered organizations with the knowledge and resources to develop, implement, manage, evaluate and optimize a comprehensive Insider Risk Management (IRM) Program (IRMP) for their organizations.

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

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

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Evaluation & Optimization Training Course (Develop, Management, Enhance)
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Customized IRM Training For Our Clients

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team 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

STUDENT / CLIENT SATISFACTION

ITDG training courses have been taught to over **1000+** individuals. Our clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM.

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

Our client satisfaction levels are in the **EXCEPTIONA**L range, due to the fact that the ITDG approaches IRM from a real world, practical, strategic, operational and tactical perspective. You are encouraged to read the feedback from our clients on this link.

COMPAY RECOGNITION

The ITDG Has Provided IRM Program Training / Consulting Services To An Impressive List Of 700+ Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(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 NITSG 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 Risk Management Program Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG