INSIDER THREAT INCIDENTS REPORT

For

Fraudulent Invoices – Shell Company Schemes

By Employees

August 2025

Produced By

National Insider Threat Special Interest Group

Insider Threat Defense Group

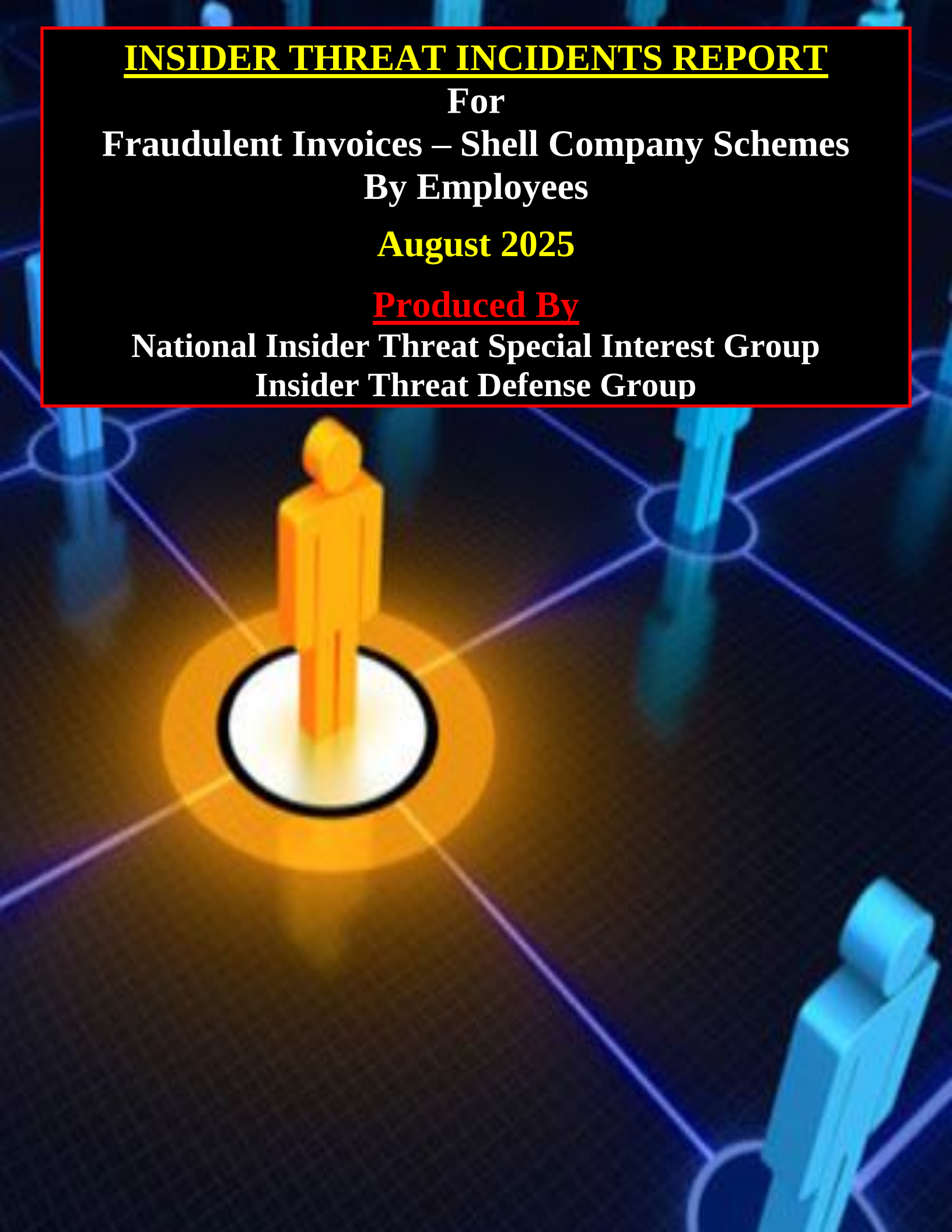


TABLE OF CONTENTS

PAGE

Fraudulent Invoices And Shell Company Schemes Overview …….. 3

Fraudulent Invoices And Shell Company Schemes Incidents …… 6

Insider Threat Definitions / Types …… 25

Insider Threat Impacts, Damaging Actions / Concerning Behaviors ....…… 26

Types Of Organization Impacted ……..... 27

Insider Threat Motivations Overview ……... 28

What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations …… 29

2024 Association Of Certified Fraud Examiners Report On Fraud …….. 30

Fraud Resources …….. 31

Sources For Insider Threat Incidents Postings ……. 32

National Insider Threat Special Interest Group Overview ……..34

Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview …… 36

FRAUDULENT INVOICES AND SHELL COMPANY SCHEMES OVERVIEW

OVERVIEW

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.

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 **6,500+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

DETECTION AND PREVENTION

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. **These fraud cases caused losses of more than $3.1 BILLION**

Recommended Controls

Verification / Certification Of Vendors / Vendor Management Policy

- ✓ A vendor verification policy is a set of procedures a company uses to ensure the legitimacy and trustworthiness of its vendors, suppliers, and other third-party providers. This policy outlines how a company identifies, assesses, and manages risks associated with its vendors / third-party suppliers. The certification of vendors will provide an additional level of confidence that the company is working with reliable and trustworthy partners.

- ✓ The company should establish a certification process for vendors against publicly available information; DUNS, Lexis Nexus, State Websites, Google Search, Addresses, Post Office Box Addresses, Etc.

- ✓ The company should regularly verify the legitimacy of vendors and ensure they are authorized to do business with the company. This can help prevent fraudulent invoicing and shell company schemes. **Cross reference employee home addresses with vendor addresses**.
- ✓ A company should have a vendor management policy and procedures that outlines how a company identifies, assesses and manages risks associated with its third-party suppliers

Key Aspects Of A Vendor Verification Policy

- ✓ **Information Gathering:**
  Initial details about the vendor, including contact information, business structure, and services offered.
- ✓ **Documentation Verification**
  Reviewing and validating documents like business licenses, registration papers, and contracts.
- ✓ **Credit And Financial Checks**
  Assessing the vendor's financial health and creditworthiness to ensure they can fulfill their obligations.
- ✓ **Compliance And Background Checks**
  Verifying adherence to relevant regulations and conducting background checks to identify any red flags.
- ✓ **Reference Checks**
  Contacting previous clients or other trusted sources for feedback on the vendor's performance.
- ✓ **Continuous Monitoring**
  Regularly reviewing vendor performance, compliance, and financial stability to proactively address any potential risks.

Vendor Management Policy Templates / Checklists / Vendor Code Of Ethics

https://frsecure.com/vendor-management-policy-template/
https://www.atgf.com/sites/default/files/forms/7000/7050.pdf
https://auracas.aura-astronomy.org/wp-content/uploads/2019/06/Vendor-Verification-Process-3.0.081319.pdf
https://www.wichitafallstx.gov/DocumentCenter/View/32899/II-7-Vendor-Verification-Policy
https://site.nyit.edu/policies/it_vendor_management_policy
https://www.process.st/templates/vendor-verification-checklist/#
https://www.spglobal.com/content/dam/spglobal/corporate/en/documents/organization/who-we-are/sp-global-vendor-code-of-conduct.pdf

Search For Information On Businesses

Open Corporates Business Search
https://opencorporates.com/advanced-search/

Lexis Nexis Business Search
https://www.lexisnexis.com/en-us/products/nexis.page

Dun & Bradstreet DUNS Number Lookup
https://www.dnb.com/duns-number/lookup.html

Dun & Bradstreet Business Directory Search
https://www.dnb.com/site-search-results.html#BusinessDirectory

Thomson Reuters CLEAR Vendor Fraud And Risk Management Solutions
https://legal.thomsonreuters.com/en/insights/articles/third-party-vendor-risk-and-compliance-management-solution
https://www.thomsonreuters.com/en/products-services/risk-fraud

Other Internal Security Controls For Fraudulent Invoices / Shell Company Schemes

- ✓ **Employee Segregation of Duties**
  Ensuring that different employees handle different aspects of the payment process to reduce the risk of fraud. (Initiate Payments, Prepare Checks, Review, Authorize, Or Sign Checks Or Approve Electronic Payments, Mail Checks, Edit Vendor Master Files, Open Mail Or Copy Checks Received And Reconcile Bank Accounts).

- ✓ **Invoice Verification Processes**
  Thoroughly verifying invoices against purchase orders, receiving reports, and other supporting documentation helps detect inconsistencies or fraudulent activity. Establish control methods to check for duplicate invoice numbers.

- ✓ **Unauthorized Changes To Payment Details**
  An employee will change payment details on an invoice for a vendor, such as bank account numbers, to divert payments to their own account.

- ✓ **Routine Audits**
  Regular audits can identify discrepancies or irregularities in financial records that may indicate fraudulent activity.

- ✓ **Technology and Automation**
  Using automated systems and data analytics can help detect anomalies, such as duplicate invoices or unusual payment patterns.

- ✓ **Employee Training and Awareness**
  Educating employees about fraud risks and reporting procedures can help encourage them to report suspicious activity.

- ✓ **Internal Controls**
  Establishing clear policies for expense and invoice processing, and requiring proper documentation for all transactions, can help deter fraudulent activity.

FRAUDULENT INVOICES AND SHELL COMPANY SCHEMES INCIDENTS

Former Miami Transit Supervisor And Wife Sentenced To Prison For Roles $75,000+ Bribery, Fraudulent Invoices & Shell Company Scheme - July 9, 2025

Dale Robinson was the acting General Superintendent and lead Rail Structure and Track Supervisor in the Track and Guideway unit of Miami-Dade Transit. His responsibilities included making recommendations for the selection of contractors to do Metrorail track maintenance and repair work for the transit unit and overseeing the work done by those contractors, including Jessie Bledsoe. Bledsoe was the co-owner and operator of JB Railroad Contracting, Inc. (JB Railroad), a North Dakota-based company that did railroad track and rail replacement, repair, and maintenance work throughout the United States.

In or around January 2021, while JB Railroad was working on a previously obtained contract for the removal and replacement of Metrorail track fasteners and was in the process of seeking an additional contract to perform welding work on the Metrorail system for Miami-Dade Transit, Dale Robinson requested a large bribe from Bledsoe. Bledsoe agreed to pay Robinson that bribe, which was intended to influence Robinson's selection of a contractor for the upcoming welding project. Bledsoe also agreed to conceal the payment by making it to a company specified by Dale Robinson.

After this, in late January 2021, Dale Robinson directed Marcia Robinson (His Wife), who lived in Maryland, to create a company and open a company checking account on which she would serve as the sole signatory. Marcia Robinson formed Tailored Railroads & Consulting LLC (Tailored Railroads), filing the company paperwork in the State of Maryland.

Between February 2021 through February 2022, Dale Robinson directed Marcia Robinson to send a total of four invoices from Tailored Railroads to JB Railroad. When Marcia Robinson sent each of these invoices, she knew that Tailored Railroads had not provided any goods or services to JB Railroad. Bledsoe then caused JB Railroad to issue four checks to Tailored Railroads to pay the invoices, which were actually payments for the bribe solicited by Dale Robinson. Bledsoe ultimately provided $75,956 to Tailored Railroads for Dale Robinson's personal benefit as part of Dale Robinson's bribe solicitation.

While not knowing all the details of her husband's illegal bribery agreement with Bledsoe, Marcia Robinson knew that the four checks were being paid by Bledsoe for Dale Robinson's recommendation to select JB Railroad to perform work for Miami-Dade Transit. Despite this, she did not inform authorities of her husband's crime, and her actions helped conceal his criminal activity. (Source)

USAID Official And 3 Corporate Executives Plead Guilty To 10 Years Bribery Scheme Involving $550 Million+ In Contracts Using Shell Companies & Fraudulent Invoices - June 12, 2025

4 men, including a government contracting officer for the United States Agency for International Development (USAID), and 3 owners and presidents of companies, have pleaded guilty for their roles in 10 year long bribery scheme involving at least 14 prime contracts worth more than $550 million in U.S. taxpayer dollars.

Roderick Watson, who worked as a USAID contracting officer, pled guilty to bribery of a public official. Other individuals involved: Walter Barnes, Darryl Britt, Paul Young.

Beginning in 2013, Watson, while a USAID contracting officer, agreed with Britt to receive bribes in exchange for using Watson's influence to award contracts to Apprio. As a certified small business under the SBA 8(a) contracting program, which helps socially and economically disadvantaged businesses,

Apprio could access lucrative federal contracting opportunities through set-asides and sole-source contracts exclusively available to eligible contractors without a competitive bid process.

Vistant was a subcontractor to Apprio on one of the contracts awarded through Watson's influence. After Apprio graduated from the SBA 8(a) program and it was no longer eligible to be a prime contractor for new contracts with USAID under this program, the scheme shifted so that Vistant became the prime contractor and Apprio became the subcontractor on USAID contracts awarded through Watson's influence between 2018 and 2022.

During the scheme, Britt and Barnes paid bribes to Watson that were often concealed by passing them through Young, who was the president of another subcontractor to Apprio and Vistant. Britt and Barnes also regularly funneled bribes to Watson, including cash, laptops, thousands of dollars in tickets to a suite at an NBA game, a country club wedding, down payments on two residential mortgages, cellular phones, and jobs for relatives. The bribes were also often concealed through electronic bank transfers falsely listing Watson on payroll, incorporated shell companies, and false invoices. Watson is alleged to have received bribes valued at more than approximately $1 million as part of the scheme. (Source)

Information Technology (IT) Shell Company Created By Employees - Shell Company Became Official Vendor For Company That Resulted In $400,000 Rip Off, And IT Equipment Had To Be Replaced (This Incident Was Provided By A NITSIG Member)

I used to work for a company who had an event precipitated by company employees in the IT department. They set up a shell company in California with the employees as the company's principle representatives.

They then applied to be an official vendor to the company that they worked for. The shell company employees then advertised that they could supply IT equipment cheaper then was commercially available. The IT folks would order from the shell company and charge full price for items that they bought off Ebay and other auction sites which was literally worn out equipment and then pocket the difference.

Someone finally researched the principle people of this shell company and discovered that they were in fact employees of the company doing business as the shell company. The result was a whole lot of terminations after a very quick investigation and the IT Department was literally gutted as a result. The CEO estimated that they had ripped him off for about $400,000 not to mention the fact that the company had to replace all the antiquated equipment that had already been installed and they also had to face a very embarrassing investigation. In the end the company chose not to prosecute due to the embarrassment that might have been publicized regarding this event. (Source NITSIG Member)

County Treasurer Sentenced To Prison For Stealing $38 Million+ In County Funds By Wiring Funds To Shell 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)

Former IT Manager Charged With $1 Million Theft & Money Laundering Scheme Using Fraudulent Invoices And Shell Company - June 24, 2025

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

Between 2016 and 2024, Richardson embezzled almost $1 million in funds from his employer through a shell corporation Richardson controlled and fraudulent invoices that billed the foundation for work not performed or performed by other vendors. (Source)

Florida Fuel Supplier For Department Of Defense Charged For Submitting Altered And Fraudulent Invoices For U.S. Navy Ships / Received $5 Million+ In Payments - June 12, 2025

Between August 2022 and January 2024, Jasen Butler, 37, of Jupiter, Florida, the owner of Independent Marine Oil Services LLC, submitted dozens of falsified documents to multiple U.S. warships, including the USS Patriot.

He demanding and received over $5 million dollars in payments for phony expenses that Butler had not incurred. These ships were attempting to purchase fuel in international ports such as Saudi Arabia, Singapore, and Croatia, among others. Butler also concealed his identity from government officials by using a false name and feigning employment by a fictitious fuel division of a different company. As alleged in the indictment, Butler used the millions in fraud proceeds to personally enrich himself and purchase multiple properties, including in Florida and Colorado. (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 company's vendor invoices were paid timely.

Martin created fraudulent vendor invoices addressed to her employer. Martin would then make unauthorized electronic funds transfers from the company's 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)

Credit Union Assistant Branch Manager Sentenced To Prison For Role In $2 Million+ Loan Fraud Scheme Using Fraudulent Invoices - June 5, 2025

Eulice Alvey pleaded guilty to conspiracy to commit bank fraud. The judge ordered Alvey to pay restitution in the amount of $2,075,458.57.

On September 6, 2018, a Neches Federal Credit Union (NFCU) member contacted the credit union and reported there were loans reflected on their account that they did not request.

Shortly thereafter, another member notified the credit union that they also had loans on their account that were not theirs. This type of notification then became common over the next few weeks, involving as many as 30 members, all associated with Billy Ray Thomas, an assistant branch manager for NFCU.

An investigation revealed Thomas was working with Alvey to commit bank fraud. Alvey would fabricate fraudulent purchase invoices for tractors from his business, Oil City Tractor, LLC, and send the invoices to Thomas. Thomas would then use credit union members' information to request a loan. Once the loan was approved, Thomas would share the proceeds with Alvey and they would use the money for personal and business ventures. In April 2025, Thomas was sentenced to 34 months in federal prison. (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:

Carmelo Marquez is a former interim Chief Security Officer for the Los Angeles County Employees Retirement Association (LACERA). He 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 under penalty of perjury.

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 under penalty of perjury 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 Charged With Embezzling $700,000+ By Creating Fraudulent Invoices And Shell Company - May 29, 2025

Jeffrey D'Souza, 68, who holds dual US and UK citizenship, is charged by indictment with seven counts of wire fraud and a two-year scheme to embezzle more than $700,000 from his employer

Between January of 2021 and December of 2022, D'Souza was employed by the victim company which did business in the District of Columbia.

D'Souza executed a scheme to defraud his company by, among other things, digitally submitting fraudulent invoices. The invoices purported to be from vendors in exchange for goods and services provided to the company.

In actuality, the fraudulent invoices included routing and account information for companies owned and operated by D'Souza which did not provide any goods or services to the victim company. Additionally, D'Souza used his access to the victim's international payroll system to direct funds into his personal accounts and the accounts of companies owned by him. (Source)

Health Foundation Executive Charged With Pocketing $1 Million+ In Kickbacks For $3.6 Million Fraudulent Invoicing 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)

Vice President Of Finance Sentenced To Prison For Embezzling $1.1 Million+ Over 11 Years By Creating Shell Company - May 15, 2025

Between October 2009 and May 2020, Kenneth Moore committed wire fraud by engaging in a scheme to embezzle $1,145,800 from his employer. Moore, who formerly held the position of Vice President of Finance, caused his employer to issue checks to "KBM Solutions," a shell company he created to receive embezzled funds. Moore laundered money by transferring the embezzled funds to his personal financial accounts.

Moore was ordered to pay $1,158,194.80 in restitution for the embezzlement scheme. (Source)

Electrical Company General Manager Sentenced To Prison For $4 Million Fraudulent Invoices Scheme Over 7 Year Period - May 15, 2025

Between July 2014 and November 2021, John Rafferty and John Pigsley defrauded Keolis Commuter Services of over $4 million through a false LJ Electric invoicing scheme.

Specifically, 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.

Rafferty then recovered the cost of these items by submitting false and fraudulent LJ Electric invoices to Keolis, which also included a percentage profit that Rafferty kept for himself.

Pigsley was ordered to pay $8,580,311 in restitution to Keolis and forfeiture of three real estate properties and a $7,687,083.70 money judgment. (Source)

Employee Admits To 9 Year International Embezzlement Scheme That Cost Employer $3.8 Million By Creating Fraudulent Purchase Orders - May 15, 2025

Bridget Thebeau admitted to embezzling from her employer from roughly January 2015 to March 2024 via more than 200 fraudulent purchase orders.

Thebeau struck a deal with some of her employer's suppliers in China in which she caused the company to pay the suppliers for products that the company did not need and never received. In exchange, Thebeau's co-conspirators in China shared the proceeds of the scam with her. Thebeau tried to hide her crime with fraudulent shipping labels and fraudulent bills of lading issued by the China-based suppliers, fraudulent invoices that she created and claimed she had issued to the company's customers and false information she supplied to the company's owner and accountants.

Ultimately, Thebeau triggered fraudulent payments of at least $3,821,152 to the company's China-based suppliers, and in return her co-conspirators wired her more than $2 million.

Thebeau was hired in 2002 by the family-owned company. Her crime resulted in substantial financial hardship to the company's owner, who is no longer able to retire due to her embezzlement, the plea agreement says. (Source)

Employee Sentenced To Prison For $4 Million+ Fraudulent Invoicing Scheme Over 5 Years - April 14, 2025

While Madelyn Hernandez was employed by a textile and apparel supply chain company, she made false and fraudulent representations to the company to obtain money. Hernandez submitted fraudulent invoices via email from purported fabric supply companies and directed payment be sent to bank accounts that she controlled. As part of her scheme, Hernandez created and submitted false invoices purporting money due and owing to a fictitious company and another that was a defunct company for goods purportedly ordered and received. As a result of her scheme, between 2018 and 2024, Hernandez received a total of $4,199,498.42 from her employer.

Hernandez's fraud came to light after the owner of the company found discrepancies in the company's financial records, including inventory discrepancies and falsified business records. In June 2024, the company became aware that invoices, proof of delivery records, and inventory reports that Hernandez had submitted were fraudulent. As the company was investigating and unraveling the fraudulent records, Hernandez sent a message to her employer from a purported family member stating that she had died after an illness and complications with surgery. The company contacted law enforcement.

In October 2024, agents with the FBI and IRS Criminal Investigation executed a search warrant at Hernandez's residence. Hernandez admitted to agents that she had emailed invoices to the company for payment and had used the money deposited into her account, held in a fictitious company name, for her own personal expenses and for gambling. Further, she admitted to sending the message to her employer stating that she had died. (Source)

Information Technology Manager Charged For Stealing $950,000+ From Employer By Creating Shell Company / Used Funds For Personal Expenses - April 11, 2025

Paul Welch worked for Algas-SDI, a energy manufacturing company, from 2011 to 2024. He was promoted to Information Technology Manager in 2018.

Welch used various schemes to steal more than $950,000 from the company.

In early 2017, Welch used the company's Amazon business account to make unauthorized personal purchases from Amazon. 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 allegedly 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 allegedly used this scheme to transfer approximately $879,175 from company accounts to his own accounts. (Source)

Former County Schools Maintenance Supervisor Pleads Guilty To $3.4+ Million Overbilling And Using - Fraudulent Invoicing Scheme - April 7, 2025

From about November 2019 through December 2023, Michael Barker ordered custodial and janitorial supplies for Boone County Schools from Jesse Marks and his company, Rush Enterprises. These supplies included hand soap, trash can liners, face masks, face shields, and hand sanitizer.

Barker admitted that he and Marks agreed that Rush Enterprises would overbill the Boone County Board of Education for these supplies. As part of this scheme, Barker approved invoices on behalf of Rush Enterprises that significantly inflated the number of products that were actually delivered to Boone County Schools. Barker submitted these fraudulent invoices to the Boone County Board of Education, which relied on them to mail checks to Rush Enterprises using the United States Mail.

Marks deposited the checks from Boone County Schools into the business bank account for Rush Enterprises, wrote himself checks on that account that he cashed at various banks, and personally delivered some of that cash to Barker in manila envelopes. Barker admitted that he spent the cash delivered by Marks to buy vehicles and equipment and make substantial improvements to his residence.

Marks deducted the cost of the products actually delivered to Boone County Schools from the proceeds of the overbilling scheme. Boone County Schools paid Rush Enterprises $4,310,714.82 from in or about November 2019 through in or about December 2023. Barker admitted that approximately 80 percent of the total payments received by Rush Enterprises, or $3,448,571.85, was based on fraudulent invoices. (Source)

Board Members For Water Works & Sewer Board And Co-Conspirators Charged In $2.4 Million Fraudulent Contractor Scheme - April 3, 2025

Criminal charges were placed against 7 defendants for a multi-million dollar fraud scheme at the Water Works and Sewer Board of the City of Prichard. in Alabama.

Starting as early as 2018 through 2022, the defendants bilked the Prichard Water Board of at least approximately $2.4 million dollars through a false and fraudulent contractor scheme involving outside contractors and employees and board members of the Prichard Water Board.

Approximately $960,000 of the money was illegally laundered, including through a business owned and operated by Nia Bradley and Randy Burden.

Ayanna Payton and another uncharged co-conspirator served on the board of the Prichard Water Board where they are alleged to have falsified payment authorizations and received kick-back payments and other benefits for their roles. Several of the conspirators communicated through coded messages and destroyed evidence to attempt to avoid detection of the crimes, according to the indictment. (Source)

Mars Wrigley Employee Charged With Stealing $28 Million By Creating Shell Company And Diverting Funds To Bank Account he Controlled - March 26, 2025

Between 2011 and 2023, Paul Steed was employed by Mars Wrigley, a subsidiary of Mars. Inc. (Mars), working remotely from his home in Stamford, Connecticut. Steed served as Global Price Risk Manager for Mars Wrigley's Global Cocoa Enterprise. As part of his employment, Steed was responsible for managing Mars Wrigley's participation in the U.S. Department of Agriculture (USDA) Sugar-Containing Products Re-Export Program.

In approximately 2016, Steed created a company, MCNA LLC, to mimic an actual Mars entity, Mars Chocolate North America.

He then diverted millions of dollars in Mars assets to a bank account he set up in MCNA's name by directing sugar refineries purchasing Mars's re-export credits, obtained through the USDA program, to pay MCNA LLC as if it were a legitimate Mars entity.

Steed is alleged to have stolen more than $28 million from Mars and through his schemes. More than $18 million was seized today for forfeiture, and the government is seeking to forfeit a Greenwich home that Steed is alleged to have purchased with nearly $2.3 million in stolen funds. It is alleged that another $2 million was sent by Steed to Argentina, where he is a dual citizen, has family ties, and owns a ranch. (Source)

Boyfriend Of A Senior Level Employee For Pharmaceutical Company Sentenced To Prison For $2.3 Million / 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.

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)

Former Assistant Chief Engineer Pleads Guilty Defrauding Company Of $8.5 Million Through Fraudulent Invoicing Scheme That Benefited 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)

Employee Sentenced To Prison For Embezzling $1 Million+ By Creating A Shell Company - December 12, 2024

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

In 2017, Alford devised a scheme to defraud his employer by creating a fake company, A&D Distributing LLC. He convinced a manager at the retailer to sell machine parts to his employer through A&D Distributing, positioning the retailer as a middleman. Alford claimed he would handle all logistics, including shipping the parts to his employer, while the retailer would simply invoice the employer for the parts, plus a profit margin.

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

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

Office Manager Sentenced To Prison For $1.3 Million Fraudulent Invoicing Scheme For Marine Forces Reserve - July 31, 2024

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

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

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

Assistant Graduate School Dean Sentenced To Prison For Role In Embezzling $1.3 Million+ Over 13 Years Using Fraudulent Invoices - December 6, 2024

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

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

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

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

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

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

The co-conspirators also used DeAlmeida's school-issued credit card to make tens of thousands of dollars in unauthorized personal purchases. For example, DeAlmeida and Martins used the card to make over $70,000 in purchases at an online retailer shipped directly to their homes, including woman's shoes, smart watches, and bed linens. DeAlmeida and Martins fraudulently altered certain receipts before submitting them to the school for payment. (Source)

Bookkeeper And Sister Sentenced To Prison For Embezzling $1.5M From Business For Fraudulent Expenses - December 5, 2024

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

Beginning in 2014, Heilman began to write checks to herself and others, to include her sister, Gray, for personal expenses. When Heilman wrote the checks to herself, and others, she made them look like legitimate business expenses on the business's general ledger. Through the course of the scheme, Heilman defrauded the company out of $1.5 million. (Source)

Company Manager Charged With Stealing $1.3 Million Using Fraudulent Invoices / Shell Companies - December 2, 2024

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

From 2021 to 2023, Laakso assumed fictitious personas and created pass-through companies, hiding these activities from GAF. He would award contracts to those fictitious companies which, in turn, would subcontract with an actual vendor to provide the product or service at a lower cost. Laakso would then keep the difference in price for his own use and enjoyment.

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

Office Of Emergency Medical Services Associate Director Sentenced To Prison For Embezzling $4 Million From Virginia Department Of Health Using Shell Company & Fraudulent Invoices / Used Funds For The Purchase Of Real Estate, Luxury Vehicles, Firearms, Jewelry - November 20, 2024

Beginning on August 10, 2013, Adam Harrell was an employee of the Virginia Department Of Health (VDH). On September 10, 2019, he became the Associate Director of the Office of Emergency Medical Services (OEMS). Harrell was responsible for managing Virginia's emergency response programs, epidemiology research, and the information technology systems that Virginia's emergency medical service providers rely on, among other responsibilities.

Harrell used his position to direct payments from VDH to a company he registered and controlled, Strategic Tech Innovations, LLC. Harrell concealed his ownership of and affiliation with Strategic Tech from VDH and OEMS, and used this entity to embezzle funds from his employer through two separate means.

From January 2021 through May 2023, Harrell created 15 fraudulent invoices for services and technology that Strategic Tech would purportedly provide to OEMS. Harrell set exorbitant and non-market prices for the various line items on the invoices, knowing the vast majority of those items would not be provided by Strategic Tech. Without OEMS's knowledge or approval, Harrell would submit these fraudulent invoices to the Western Virginia EMS Council (WVEMS), a regional emergency medical services council that serves as a pass-through for OEMS payments to vendors. Each of these invoices were paid by WVEMS with OEMS funds. By directing the invoices to WVEMS instead of Accounts Payable at OEMS, Harrell circumvented the requirement that Strategic Tech be approved as a vendor to VDH and OEMS and evaded scrutiny by the Accounts Payable department. As the Associate Director of OEMS, Harrell was able to unilaterally approve the same fraudulent Strategic Tech invoices he drafted.

Harrell deposited each of the checks he illegally received from WVEMS into the Strategic Tech checking account he controlled. In total, Harrell received $4,337,395 in OEMS funds.

The Consent Order of Forfeiture imposed not only a monetary judgement for the full proceeds Harrell obtained, but also called for the forfeiture of assets purchased using the proceeds, including real estate, vehicles, approximately 95 assorted firearms, a Rolex Submariner stainless steel wristwatch, a TAG Heuer Connected Steel watch, a Breitling Navitmer chronograph watch, a 14K princess cut white gold diamond stud earrings, and proceeds from the sales of certain assets. (Source)

Assistant Treasurer For Bridgestone Tires Charged With $15 Million Wire Fraud - Money Laundering Scheme Using Shell Company & Fraudulent Invoices - November 12, 2024

Starting in 2016, Sajju Khatiwada was employed by Bridgestone in various positions, and he was working as Bridgestone's Assistant Treasurer, Capital Planning and Funding, when he left the company in April 2024. Khatiwada was responsible for managing the relationships with banks that provided credit card processing services at each of the retail Bridgestone locations across the United States, acting as a liaison with bank representatives and initiating payments for bank fees and credit card processing fees.

In July 2020, Khatiwada created a phony vendor called Paymt-Tech, LLC and began submitting bogus invoices to Bridgestone for purported bank fees owed to Paymt-Tech. Each month from August 2020 to April 2024, Khatiwada sent an email from his Bridgestone email account to initiate a payment to Paymt-Tech, LLC for the fictitious monthly bank fees. The email would contain a bogus PDF invoice and would request payment of the invoice. Bridgestone approved payment of these invoices, believing they were for true bank fees for a legitimate vendor, Chase Paymentech.

In April 2024, Khatiwada left his employment at Bridgestone. Approximately two months later, Bridgestone Accounting Department personnel questioned the significant decrease in monthly bank fees being paid by Bridgestone. The subsequent investigation identified that between August 2020 and April 2024, Khatiwada had submitted 47 false invoices to Bridgestone for a total amount paid of $14,923,978.57, which the FBI traced back to Khatiwada. (Source)

Pharmaceutical Company IT Employee Sentenced To Prison For Embezzling $2.5 Million Using Shell Company & Fraudulent Invoices - October 31, 2024

Between January 2022 and October 2022, Priya Bhambi and her alleged co-conspirator orchestrated and executed a scheme to defraud Takeda Pharmaceutical Company 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, the co-conspirator, in coordination with Bhambi, allegedly incorporated 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, allegedly in coordination with the co-conspirator, 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 the alleged co-conspirator fabricated and submitted to Takeda five separate invoices for services that Evoluzione had not performed, each in the amount of $460,000. When questioned by Takeda employees, Bhambi and the alleged co-conspirator 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 allegedly opened by the alleged co-conspirator in the name of Evoluzione.

Bhambi was also ordered to pay $2,585,480 in restitution. Bhambi was ordered by the court to forfeit a Mercedes-Benz Model E, over $1 million in fraud proceeds held in bank accounts and a $49,985 wedding venue deposit, all seized by the government, as well as a diamond engagement ring and a Seaport condominium purchased with fraud proceeds. (Source)

Former Williams-Sonoma Warehouse Manager Charged With Stealing $10 Million By Using Shell Company & Fraudulent Invoices / Used Funds For Purchasing Home, Yacht, Automobiles, Sporting Tickets, Etc. - September 19, 2024

Ben Thomas is a former employee of San Francisco based Williams-Sonoma. He was charged on with defrauding the company more than $10 million.

Thomas is alleged to have registered a fake company called Empire Logistics Services (Empire) billing Williams Sonoma, Inc. millions of dollars for work that Empire never performed, according to the indictment.

Thomas allegedly spent the money on a yacht, automobiles, sporting events tickets, pet cloning, a 12,000-square-foot home, and professional landscaping services for the home.

Thomas worked as a General Manager at a Williams-Sonoma hub and distribution facility in Braselton, Georgia from 2016-2023.

From 2017-2023, he allegedly submitted hundreds of Empire invoices to Williams-Sonoma, each one under his $50,000 approval limit, and approving them.

During that time, Thomas made 335 payments totaling $10 million to a bank account he managed. (Source)

Company Credit Analyst Pleads Guilty To Embezzling $1.4 Million+ By Directing Vendor Payments To His Personal Banking Account - September 10, 2024

Adil Rahman worked in Ontario, Canada as a credit analyst for Company A, that was a subsidiary of a large electrical distribution and services company based in Pittsburgh. As part of his job, Rahman interacted with clients of Company A concerning invoices for the company's services. Between November 2022 and December 2023, Rahman directed certain customers of Company A to pay their invoices via ACH transfers to his personal bank account, rather than to the account of Company A.

For example, in or about November 2022, Rahman sent an email to the accounts payable department of Company B – a nonprofit municipal corporation based in Hartford, Conn. asking if the company would be interested in paying future invoices to Company A by ACH transfer rather than by check. When Company B agreed to do so, Rahman provided his personal account information to Company B. Thereafter, under the false impression that it was sending the money to Company A to pay the invoices it owed, Company B sent at least 15 ACH transfers to Rahman's personal account between December 2022 and June 2023.

In May 2023, Rahman emailed the accounts payable department at Company C, a privately held provider of corporate security systems based in Andover, Massachusetts, asking if Company C wished to pay future invoices by ACH transfer.

Once again, when Company C agreed to do so, Rahman provided his personal bank account information and Company C thereafter made 11 ACH transfers to Rahman's personal account between May 2023 and July 2023.

In total, through this scheme, Rahman defrauded Company A and its clients of more than $1.4 million. (Source)

Employee Sentenced To Prison For Stealing $1.2 Million+ Using Fraudulent Invoices, Fake Employees & Impersonating Employees Over Zoom - July 31, 2024

Caleb Keller began working for his employer in 2011, soon after graduating college.

Between April 2017 and June 2021, Keller created and submitted 101 false and fraudulent invoices to his former employer through his side business, Polyglot Developers. After arranging for his employer to contract with Polyglot, he created two fictitious employees, "Matt Pearson" and "Grant Miller." He then drafted false invoices that billed his employer for services allegedly performed by the two fake employees.

For example, on April 29, 2019, Keller submitted a $19,940 invoice to his employer for services allegedly rendered by four employees, including $15,200 for services allegedly rendered by the two fictitious employees. When an executive at his employer became suspicious of the fake employees and demanded a meeting with "Matt Pearson," Keller pretended to be Pearson on a Zoom call by using a video filter. During the meeting, it became obvious that Pearson was not real and that the person purporting to be Pearson was actually Keller. Following the meeting, Keller was fired and his employer's relationship with Polyglot was terminated. In April 2022, Keller was interviewed by law enforcement investigators and insisted that Pearson and Miller were actual employees who provided services to his employer.

In July 2022, Keller was interviewed again and admitted that the purported employees were fake and that he had impersonated Pearson on the Zoom call.

Due to this years' long scheme, Keller's employer was deceived into paying Keller approximately $1,210,120 for work they believed was completed by fictitious employees of Keller's business. Keller used the fraudulently obtained money to pay for personal expenses. (Source)

Assistant Vice President For Insurance Company Admits To $1 Million Shell Company Fraud Scheme / Received $350,000 In Kickbacks From Vendors - July 30, 2024

James Keating was an Assistant Vice President and surety bond claims handler at Allied World Insurance Company (Allied World). He later served in the same capacity at Crum and Forster subsidiary U.S. Fire Insurance Company, where he also handled claims on Allied World surety bonds. All surety bond claims were handled through Allied World's offices in Farmington, Connecticut.

Between 2017 and 2021, Keating defrauded Allied World in two ways. First, he used a shell company, American Construction & Industrial LLC, to bill Allied World for unnecessary claims work that was not performed and took the proceeds for himself. Second, he solicited and received kickbacks from Allied World vendors through another Keating-owned company, Surety Risk Solutions, without the knowledge of his employer. Keating also caused these vendors to use another company in which he had an undisclosed ownership interest, Kodiak Asset Recovery, for asset searches at vastly inflated prices. Keating profited nearly $1 million through American Construction & Industrial LLC, more than $350,000 in kickbacks.

Keating has agreed to pay restitution of $1,226,603.97, which represents the loss to Allied World of $1,446,491.95, less $219,887.98 that he previously repaid as part of a civil judgment. (Source)

Company Operations Manager Pleads Guilty To Embezzling $1.49 Million+ Over 7 Years Using Fraudulent Invoices / Used Funds For Mortgage Payments, Car Loans, Vacation, Etc. - July 18, 2024

From 2004 to 2020, Gabriel De Chavez worked as an Operations Manager.

Between 2012 and 2019, De Chavez used his position to generate fake invoices purportedly created by genuine vendors for goods and services. He presented these fake invoices and corresponding checks made out to the real vendors to his employer for signature, and would then deposit the checks into his own personal bank account.

De Chavez used the funds to pay for personal expenses including credit card payments, cash withdrawals, mortgage payments, vacations, and car loans. He was able to continue the scheme without notice because of the trusted position he held at the company. Between 2012 and 2019, Ruiz De Chavez created over 600 fake invoices and checks, causing at least $1,491,000 to be transferred into his account from his employer.
(Source)

Defense Of Department Employee Pleads Guilty To Stealing $624,000+ Using Fraudulent Invoices - July 1, 2024

Zelene Charles, a previous civilian employee of the Department of Defense, at the Defense Language Institute in Monterey, California, perpetrated a scheme to defraud the U.S. government by creating fake purchase requests and invoices for government purchases from both fictitious and legitimate business entities.

The items listed in these invoices were never actually purchased or received by the government.

Between December 2016 and April 2020, Charles placed approximately 185 fraudulent charges, causing a total loss to the government of $624,250. To conceal that she was the recipient of the stolen funds, Charles frequently renamed the business names associated with intermediary accounts and, in total, used at least 78 different account names. (Source)

IT Systems Engineer Sentenced To Prison For Embezzling $526.0000+ Using Fraudulent Invoicing Scheme For 11 Years - May 31, 2024

Scott Richard was a systems engineer for Company A. He was entrusted with the specification, purchase, installation, and support of equipment and systems used by the company's technology infrastructure.

Richard admitted to fraudulently using the corporate credit card issued to him by Company A for his own personal benefit. Richard embezzled money from his employer by creating false invoices for a shell company he controlled and using his corporate card to make fraudulent purchases from the shell company.

Richard also made unauthorized purchases of equipment, for his own personal use, with his corporate card. From January 1, 2012 through September 27, 2021, Richard fraudulently diverted $526,569.42 from Company A to himself. (Source)

Former U.S. Department of Agriculture Program Director & Nephew Arrested For $400,000 Fraudulent Contracting Scheme / $125,000 Kickback Scheme - May 22, 2024

From August 2015 through November 2022, Kirk Perry, a United States Department of Agriculture (USDA) Program Director, arranged for Jamarea Grant (Perry's Nephew) to be hired by two companies under contract with the USDA Office for Civil Rights.

Grant reported directly to Perry, and the two of them conspired to bill the government for work that Grant did not actually perform. Grant is alleged to have received nearly $400,000 for work he did not do, and, in return, kicked back approximately $125,000 to Perry as part of the criminal scheme. (Source)

Outside Individual Found Guilty For Role In Defrauding Company Out Of $5.8 Million Using Fake Invoice Scheme For 18 Years / Was In Collusion With IT Director - May 14, 2024

From February 2000 to April 2018, Kevin Horton schemed with Tony Rawlings, the Information Technology (IT) Director at Melissa's World Variety Produce Inc., to defraud Melissa's out of its money through the approval of payment of invoices for IT services that were never provided.

Horton created a shell company called Creative Network Solutions (CNS), whose purpose was to send fraudulent bills to its sole client, Melissa's. In consultation with Rawlings, Horton created two fictitious invoices per month, in which CNS billed Melissa's for IT services that CNS did not provide, for approximately 18 years, through February 2018.

Horton provided the fictitious invoices to Rawlings, who approved them, vouched for their operational necessity, and then forwarded them to a Melissa's executive who was asked to have Melissa's pay CNS the amounts listed on the sham invoices.

Horton, along with Rawlings, caused Melissa's to send CNS payment in the form of checks mailed through the U.S. Mail to a post office box to which Horton had sole access. Horton deposited the checks he received through the scheme into a bank account that he exclusively controlled. Horton then funneled Rawlings a portion of the money that Melissa's paid to CNS, in the form of checks sent via U.S. Mail to addresses where Rawlings lived.

In total, Horton, along with Rawlings, caused Melissa's to pay CNS approximately $5,852,604 because of the fictitious invoices (Source)

2 Executives Sentenced To Prison For Roles In $4 Million Fraudulent Vendor - Invoicing Scheme - April 30, 2024

Shawn Rains and Joseph Maharaj were sentenced to prison, for their participation in a scheme to steal millions of dollars from a company where they were formerly high-ranking executives.

Rains and Maharaj designed and executed a scheme to defraud OrthoNet of over $4 million and to launder the fraud proceeds. Rains and Maharaj conspired with others to create fake vendors that purported to do work on behalf of OrthoNet. Rains, Maharaj and their co-conspirators then signed invoices approving payment for the fake work, and OrthoNet sent payments to the fake vendors.

Rains, Maharaj and their co-conspirators then converted the money to cash to hide the source of the fraud proceeds and split it up amongst themselves. (Source)

Men's Wearhouse Company Employee Pleads Guilty To Embezzling $1.7 Million Over 8 Years By Creating Fraudulent Invoices / Shell Company - September 19. 2023

Gina Lone star was a Director in the Facilities Department of Men's Wearhouse. She was promoted to Senior Director of Facilities and Corporate Services and then to Vice President of Construction, Maintenance, and Facilities.

Gina Lonestar admitted that, in December 2010, she devised a scheme to create a fake vendor to defraud Men's Wearhouse and later Tailored Brands (Men's Wearhouse's parent company) of money by submitting and approving false invoices for the fake vendor to the accounts payable department.

Lonestar created a document stating the vendor was a sole proprietorship associated with a family member and then began submitting and approving invoices falsely claiming the vendor was performing work at Men's Wearhouse stores throughout California, such as inspections and handyman work.

Lonestar admitted that she submitted and approved false invoices in the name of the fake vendor for approximately eight years, defrauding her employer of over $1.7 Million, which was paid to her joint checking account. Lonestar admitted that the vendor did not exist and the family member with whom she co-owed the company performed none of the work for which she provided invoices.

In all of her roles, she had the authority to approve invoices for work done by vendors. Lonestar's scheme ended in 2019 when the company discovered the conduct during an internal audit. (Source)

Company Former Accounting Manager Sentenced To Prison For Embezzling $2.5 Million+ Over 8 Years By Creating Shell Company / Used Funds For Drug Addiction - August 29, 2023

Christin Guillory was an Accounting Manager at an manufacturing company. She stole more than $2.5 Million from her employer by transferring funds to accounts Guillory set up in the names of fake companies and then routing the funds to her own bank accounts.

In April 2013, Christin Guillory set up an account with payment processor Square that used a display name that made it appear it was an account of a commercial shipping company.

Between 2014 and 2019, Guillory secretly paid $1,695,591 to that account and then transferred the money to her own bank accounts. She made false entries in the company books to conceal the theft.

In 2019, Guillory stopped using Square for her fraud and instead used two PayPal accounts. She gave one of the PayPal accounts a display name similar to that of her employer. For the second account, she used the name of a shipping company with which she had no affiliation. In 2020 and 2021, she caused the transfer of $604,000 to the PayPal accounts and made false accounting entries to cover her tracks. She then transferred the bulk of the money for her own use. Becoming more brazen, between August and November 2021, Guillory transferred $247,000 directly from company accounts to her own bank accounts. Again, she made fraudulent accounting entries and reused legitimate invoices to make it appear the payments were for appropriate business purposes. In all, Guillory made at least 867 secret transactions using interstate wires that totaled $2,536,086.

Guillory used the stolen money to support her prescription drug addiction. The scheme was detected when a financial institution reported irregularities. (Source)

Amazon Manager Sentenced To Prison For As Mastermind In $10 Million Fraudulent Invoicing Scheme - July 5, 2023

Kayricka Wortham abused her position at Amazon to submit more than $10 Million in fictitious invoices for fake vendors, causing Amazon to pay approximately $9.4 million to Wortham and her other 6 co-conspirators.

From about August 2020 to March 2022, Wortham worked as an Operations Manager at the Amazon Warehouse in Smyrna, Georgia. In her position, Wortham supervised others and acted with the authority to approve both new vendors and the payment of vendor invoices for Amazon.

Wortham, who was the leader of the scheme, provided fake vendor information to unknowing subordinates and asked them to input the information into Amazon's vendor system. Once the information was entered, Wortham approved the fake vendors, enabling them to submit invoices.

Wortham and co-conspirators then submitted fictitious invoices to Amazon, falsely representing that the vendors had provided goods and services to Amazon. Wortham approved the invoices, causing Amazon to transfer millions in fraudulent proceeds to bank accounts controlled by her and her co-conspirators.

Wortham conspired with others, including Brittany Hudson, in the scheme. Hudson was in a relationship with Wortham and owned a business. Hudson allegedly worked with Wortham to submit millions in fictitious invoices for fake vendors to Amazon. Wortham and Hudson purchased expensive real estate and luxury cars, including a nearly $1 Million home in Smyrna, Georgia, a 2019 Lamborghini Urus, a 2021 Dodge Durango, a 2022 Tesla Model X, a 2018 Porsche Panamera, and a Kawasaki ZX636 motorcycle, all with fraudulent proceeds from the scheme.

Wortham also recruited co-conspirators Demetrius Hines, who was in Loss Prevention at Amazon, and Laquettia Blanchard, who worked as a Senior Human Resources Assistant at the company. Hines also recruited Jamar L. James, Sr., another Operations Manager at Amazon's location in Duluth, Georgia, into the scheme. Like Wortham, James allegedly approved fake vendors and fictitious invoices, including after Wortham left Amazon in March 2022. (Source)

Apple Employee (Purchasing Agent) Sentenced To Prison For Defrauding Apple Out Of $17 Million By Taking Kickbacks From Vendors, Inflating invoices & Stealing Parts - April 26, 2023

The criminal conduct in this case centered around Dhirendra Prasad's employment at Apple from December 2008 through December 2018. For most of that time, he was a "buyer" in Apple's Global Service Supply Chain. It was Prasad's job as an Apple buyer to facilitate the process through which Apple bought parts to perform warranty repairs on older devices.

Prasad exploited his position and conspired with two separate Apple vendors to defraud Apple by taking kickbacks, stealing parts, inflating invoices, and causing Apple to pay for items and services it never received – resulting in a loss to Apple of more than $17,000,000. (Source)

And Many More…….

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

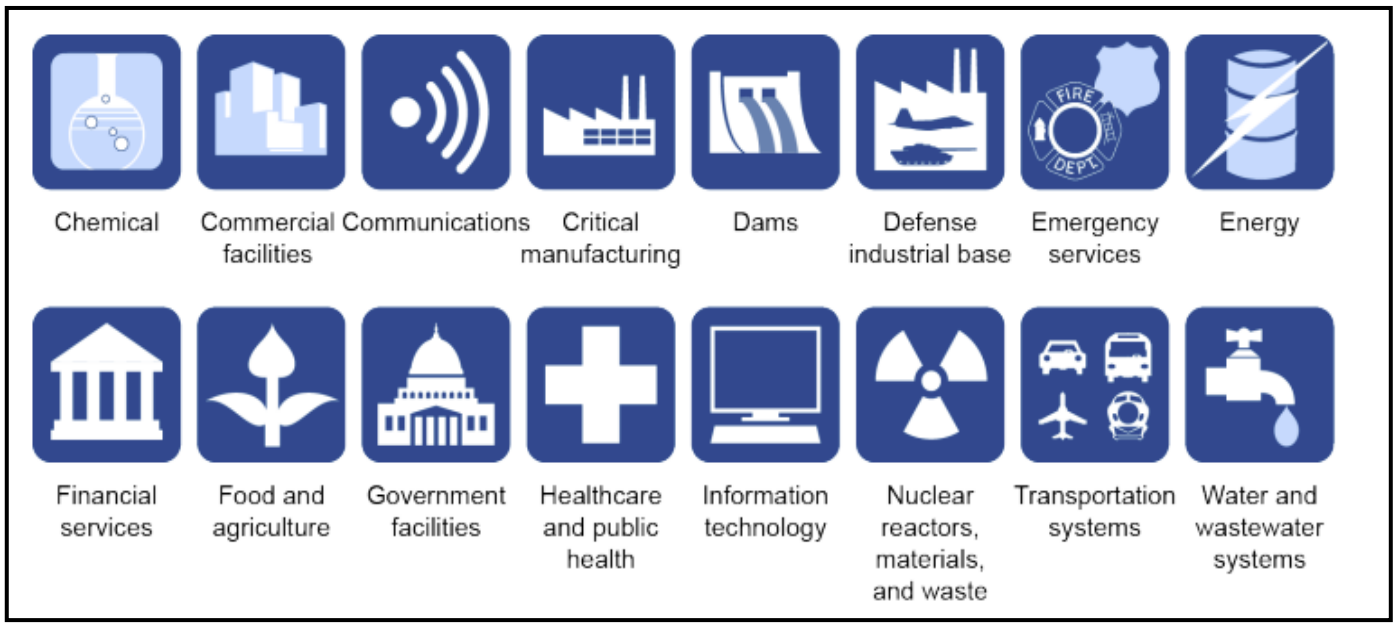
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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

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

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

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

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

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

Can your organizations Network Security / Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for products or services that are were 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.

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 (**6,500+ Incidents**).

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

https://twitter.com/InsiderThreatDG

Follow Us On Twitter: @InsiderThreatDG

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**

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

SPECIALIZED REPORTS

Why Insider Threats Remain An Unresolved Cybersecurity Challenge

Produced By: IntroSecurity And NITSIG / 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'

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 happy 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