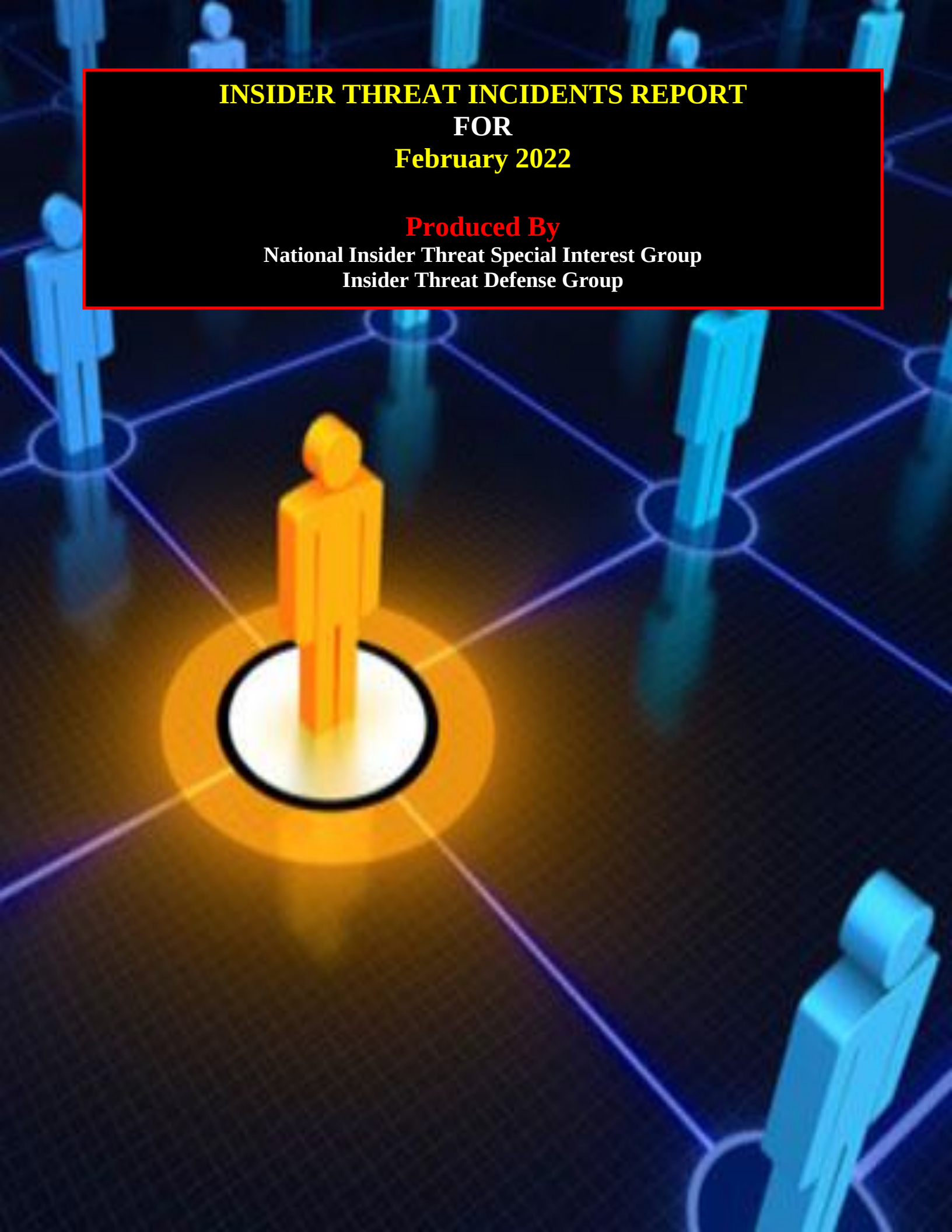

INSIDER THREAT INCIDENTS REPORT
FOR
February 2022

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **3,300+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees.

According to the Association of Certified Fraud Examiners 2020 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

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

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 21 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM CC2 & Other Sources) and be expanded.

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

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR FEBRUARY 2022

U.S. GOVERNMENT

Former FBI Special Agent Pleads Guilty To Misusing $13,500 For Blackjack Gambling Using Government Funds - February 23, 2022

From July 27 to July 31, 2017, Scott Carpenter while employed as a Special Agent with the FBI's New York City Field Office, he and 3 other FBI agents traveled to Las Vegas to conduct an undercover operation.

At the conclusion of the operation, Carpenter went to a casino's high limit room, where he gambled on blackjack with $13,500 belonging to the United States. (Source)

U.S. Postal Service (USPS) Employees Involved In Stealing Mail As Part Of $366,000 Bank Fraud Scheme - February 14, 2022

From February 2019 to May 2020, Jeffrey Bennett conspired to fraudulently obtain money from victim financial institutions by depositing counterfeit checks and checks stolen from the mail into accounts at these financial institutions and withdrawing funds before the financial institutions identified the fraudulent checks and blocked further withdrawals.

Bennett and his conspirators arranged for U.S. Postal Service (USPS) employees to steal credit cards and blank check books from the mail in exchange for cash payments. USPS employees provided the checks to Bennett and his conspirators, who forged the signatures of the accountholders and negotiated the checks by making them payable to individuals, some of whom were New Jersey high school students, who had given Bennett and his conspirators access to their accounts, also in exchange for cash. Bennett and his conspirators obtained and attempted to obtain approximately $366,000 from victim financial institutions. (Source)

Former United States Postal Service Employee Sentenced To Prison $232,000+ Bank And Mail Fraud Conspiracy - February 18, 2022

Johnson Ogunlana was a letter carrier for the U.S. Postal Service (USPS).

Between July 25, 2016 and February 5, 2019, Ogunlana, and his co-conspirator Samson Oguntuyi, conspired with others to steal bank checks and credit and debit cards from the mail, open fraudulent business banking accounts using the names of victim businesses and the stolen identities of victim postal customers to negotiate the stolen checks by depositing them into the fraudulent bank accounts, and then conduct transactions with stolen payment cards and with money derived from the stolen checks.

Ogunlana has been ordered to pay $232,588 in restitution. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Metallurgist Lab Director Pleads Guilty To Falsifying Test Results For Strength Of U.S. Navy Submarines Hulls - February 14, 2022

Bradken, Inc. is the U.S. Navy's leading supplier of cast high-yield steel for naval submarines. Bradken's Tacoma foundry produces castings that prime contractors use to fabricate submarine hulls. The Navy requires that the steel meets certain standards for strength and toughness to ensure that it does not fail under certain circumstances, such as a collision. For 30 years, the Tacoma foundry (which was acquired by Bradken in 2008), produced castings, many of which had failed lab tests and did not meet the Navy's standards.

Elaine Thomas, as Director of Metallurgy, falsified test results to hide the fact that the steel had failed the tests. Thomas falsified results for over 240 productions of steel, which represent a substantial percentage of the castings Bradken produced for the Navy.

Court filings indicate there is no evidence that Bradken's management was aware of the fraud until May 2017. At that time, a lab employee discovered that test cards had been altered and that other discrepancies existed in Bradken's records.

For 32 years, Elaine Thomas betrayed the trust of the United States Navy, knowingly placing its sailors and military operations at risk," said U.S. Attorney Nick Brown. "She falsely stated that steel Bradken produced met critical specifications– standards developed to keep our military personnel safe– and allowed inferior steel to go to Navy subs in half the orders she reviewed. (Source)

U.S. Navy Commander Pleads Guilty In Navy Bribery Scandal Involving Extravagant Dinners, Hotels, Parties & Prostitutes From Foreign Defense Contractor - February 2, 2022

Former U.S. Navy Captain Donald Hornbeck pleaded guilty to bribery charges, admitting that while he directed the operations of all combatant ships in the Seventh Fleet, he accepted at least $67,830 in extravagant dinners, hotels, parties and prostitutes from foreign defense contractor Leonard Francis in exchange for breaching his official duty to the U.S. Navy.

Hornbeck admitted that he corruptly used his official position to benefit Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia (GDMA). GDMA serviced U.S. Navy ships in the Asia Pacific region. Hornbeck admitted that he endeavored to send Navy ships into ports serviced by GDMA; shared confidential Navy information with Francis in order to help GDMA; and helped with evaluating and indoctrinating potential new Navy members to help Francis.

Hornbeck was one of nine members of the U.S. Navy's Seventh Fleet indicted by a federal grand jury in March 2017 for conspiring with Francis and for receiving bribes. Many other Navy personnel are also involved. (Source)

Nuclear Engineer Pleads Guilty To Espionage Involving Design Data For Nuclear Powered Warships - February 14, 2022

Jonathan Toebbe, was arrested on Oct. 9, 2021, after he placed an SD card at a pre-arranged dead drop at a location in West Virginia.

Toebbe was an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program. He held an active national security clearance through the Department of Defense, giving him access to Restricted Data.

Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships. (Source)

Wife Of Nuclear Engineer Pleads Guilty To Espionage Related Offense - February 18, 2022

Diana Toebbe was arrested on Oct. 9, 2021, for knowingly and voluntarily joining a conspiracy with her husband, Jonathan Toebbe, to communicate Restricted Data to a foreign nation. During the course of the conspiracy, Diana Toebbe served as a lookout while her husband serviced three "dead-drops."

Jonathan Toebbe was an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program. Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships.

Jonathan Toebbe sent a package to a foreign government, listing a return address in Pittsburgh, Pennsylvania, containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Jonathan Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was really an undercover FBI agent. Jonathan Toebbe continued this correspondence for several months, which led to an agreement to sell Restricted Data in exchange for thousands of dollars in cryptocurrency. (Source)

Construction Company CEO Admits To Bribing Army Biochemist Researcher For Government Contracts By Financing 2 Rental Properties - February 25, 2022

John Conigliaro is the owner and Chief Executive Officer of EISCO, Inc. EISCO provides general construction services, including fixed and portable biochemical laboratories.

According to his guilty plea, from 2012 to 2019, Conigliaro bribed an Army Research Biologist, who worked at the U.S. Army Combat Capabilities Development Command (CCDC) Chemical Biological Center (CB Center), located on Aberdeen Proving Ground, in Maryland.

Conigliaro the Army Research Biologist with a stream of benefits including cash loans, payments for renovations to rental properties, payments for renovations to his personal residence, and other things of value in exchange for influencing CB Center projects to EISCO.

In October 2013, after EISCO received its first payment of $150,000 for a government project, Conigliaro gave cash and a $40,000 zero-interest loan to the Army Research Biologist
to finance the purchase of two rental properties. Conigliaro paid for thousands of dollars of renovations to the rental properties.

Additionally, from 2016 to 2018, the Army Research Biologist directed three CB Center projects to EISCO. During the performance of one of those projects, Conigliaro spent approximately half of the time not performing work but being "on call." Conigliaro paid for more than $30,000 in renovations to his personal residence, including more than more than $20,000 to renovate the kitchen, and more than $16,000 to replace the siding on his personal residence.

From July 2012 to 2019, Conigliaro paid more than $95,000 in bribes to the Army Research Biologist, and over that same time period, Army Research Biologist directed more than $1 million of contract awards to EISCO. (Source)

Former Veterans Affairs Medical Center (VAMC) Employee Sentenced To Prison For Stealing $8.2 Million+ Worth Of HIV Medication - February 24, 2022

From August 2017 through Nov. 20, 2019, Wagner Checonolasco conspired with Lisa M. Hoffman and others to steal HIV medication belonging to the U.S. Department of Veterans Affairs.

Hoffman allegedly stole the medication from the pharmacy of her employer, the Veterans Affairs Medical Center (VAMC) in East Orange, New Jersey, and then sold the stolen medication to Checonolasco for cash.

Hoffman used her position as a procurement official at the VAMC to order large quantities of HIV prescription medications so that she could steal the excess medication and then sell it to Checonolasco, who then resold it for a profit. Checonolasco and Hoffman stole approximately $8.2 million worth of HIV medication belonging to the VAMC. (Source)

Former Ft. Bragg Employee Pleads Guilty To Accepting $1 Million In Bribes Over 8 Years - February 16, 2022

Calvin Jordan was a procurement agent assigned to the Operations and Maintenance Division, Directorate of Public Works (DPW), at Fort Bragg, NC.

From 2011 into 2019, Jordan used his position as a procurement agent to receive bribes of approximately $200 per DMO from various vendors contracting with DPW, Ft. Bragg, North Carolina, in return for increasing the amount of federal contracts given the vendor. Jordan received approximately $1 million in illegal bribes. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former Special Inspector For New York Metropolitan Transportation Authority Sentenced To Prison For $5.6 Million+ COVID-19 Relief Fraud - February 24, 2022

Sean Andre was sentenced to prison for conspiring with another man to fraudulently obtain more than $5.6 million in government-backed loans meant for businesses struggling with the financial effects of the coronavirus pandemic.

Andre admitted to helping Jean Lavanture obtain $4,309,581 in Paycheck Protection Program (PPP) loans between June and August 2020, by submitting fraudulent loan applications in the names of four companies that Lavanture controlled. Each loan application misrepresented the number of employees, and total payroll, that each company had, and included false tax documents that Andre created as part of the scheme. Andre was paid $157,578 for his role in the scheme.

Andre also admitted that he fraudulently obtained an additional $1,309,754 in pandemic relief loans, by submitting loan applications in the names of companies he controlled. In these loan applications, Andre lied about the number of employees, and total payroll, that his companies had. (Source)

Former California Employment Development Department Employee Sentenced To Prison For Fraudulently Obtaining Nearly $4.3 Million In COVID Relief Funds - February 4, 2022

From April to October 2020, Gabriela Llerenas filed fraudulent unemployment insurance benefits claims, that falsely asserted the named claimants were self-employed independent contractors, often identifying them as cake decorators or event attendants, who were negatively affected by the COVID-19 pandemic.

Llerenas also falsely stated on some of the applications that the claimants were residents of California entitled to unemployment insurance benefits administered by EDD when in fact they lived elsewhere. On some applications, she inflated the amounts of income she reported for the claimant to maximize the benefit amount. She also filed a dozen or more fraudulent EDD claims in a day.

Llerenas obtained some of the names, Social Security numbers and other identifying information she used to submit the fraudulent claims through her prior work as a tax preparer.

Llerenas charged the named claimants a fee for filling the applications, which was often paid out of the fraudulently obtained benefits. In at least one case, she told the named claimant that she was still employed at EDD and could control the distribution of the unemployment insurance benefits, and then demanded an additional payment for "releasing" the benefits.

In total, 197 debit cards were fraudulently issued because of this schemes Llerenas submitted nearly 200 fraudulent COVID-related unemployment relief claims to be filed in other people's names, resulting in nearly $4.3 million in ill-gotten gains.

Llerenas previously worked at EDD as a disability insurance program representative. She resigned in March 2002 after admitting to fraudulently authorizing and paying disability benefits administered by EDD. She was sentenced to 37 months in federal prison in connection with that scheme. (Source)

Former County Deputy Clerk Convicted In $1.3 Million Fraud Scheme, Co-Defendants Plead Guilty To Related Charges - February 1, 2022

Willie Demps worked for the Muscogee County Clerk for approximately 30 years and supervised money deposits received by the Clerk's Office. The Clerk's Office received money from fines and condemnations, and payments were frequently made in cash.

From at least 2010 to 2019, Demps maintained a safe in his office to store sums of cash that were collected by the Clerk's Office. During the business day, this safe was rarely locked, even when Demps was away from his office. Demps (or his designee) was responsible for depositing cash received by the Clerk's Office into an appropriate Clerk of Superior Court bank account. Records indicate that the Clerk's Office received over $5.5 million in cash during the period of 2010-2019, yet only a single cash deposit of approximately $210 was made into official Columbus accounts in 2019. No cash deposits were made in other years.

From Oct. 19, 2010, to approximately Nov. 27, 2019, Demps issued at least 330 Clerk of Superior Court checks payable to the named co-defendants, and to some individuals not named, with a face value of at least $1.3 million. Demps would meet various co-defendants in locations away from his place of business at the Clerk's Office to give the illicit checks to them to be cashed at banks in Columbus and in nearby Alabama. The co-defendants cashed the checks and returned the money to Demps, who would give the participating co-defendant a portion of the money. Demps admits he used the money for personal expenses, to send money to foreign countries and to spend at casinos. (Source)

Richmond Community College Director Charged With Stealing Student Financial Aid Funds Over 6 Years - February 2, 2022

From 2006 through 2017, Kiesha Pope, was the Director of Financial Aid at J. Sargent Reynolds Community College (JSRCC), a public community college servicing the greater Richmond area.

Pope is alleged to have used her access to financial aid systems at JSRCC to boost the financial aid eligibility for co-conspirators, who were Pope's friends and family members and who were not otherwise eligible for financial aid benefits at JSRCC. Pope allegedly had agreements with these same co-conspirators to receive a portion of the improperly obtained financial aid funds as compensation. Pope is alleged to have spent these financial aid funds on various of her personal expenses, including repairs for her personal vehicle, retail shopping, and expenses for her minor-aged daughter.

From 2011 to 2017, Pope procured financial aid for her son, knowing that he was not attending JSRCC in this timeframe. In another instance, Pope also allegedly procured financial aid for her ex-fiancé from in or about 2010 through in or about 2015 while he was serving a term of incarceration and not attending JSRC. To conceal her scheme, Pope allegedly falsified supporting justification for the financial aid. In one alleged instance, Pope forged medical documents and financial aid documents reflecting that her goddaughter, for whom Pope also procured financial aid, was failing to meet academic eligibility due to a breast cancer diagnosis, despite knowing that her goddaughter had no cancer diagnosis. (Source)

Former School District Assistant Superintendent Convicted In $28,000 Bribery Scheme - February 7, 2022

Jose Morin was the former La Joya Independent School District (LJISD) assistant superintendent of Student Services.

Morin admitted to receiving approximately $28,000 as bribes beginning in 2019 for his official and favorable recommendations at LJISD. They pertained to energy savings contracts awarded to a company as well as job order contracts and facilitating the processing of pay applications related to those contracts. The LJISD school board subsequently approved the contracts Morin recommended. (Source)

Former University Of Pittsburgh Director Of Emergency Management Admits To Stealing & Selling PPE Masks - February 9, 2022

PayPal informed the FBI that a vendor on Ebay known as Steel-City-Motor-Toys sold over 13,000 PPE, primarily Aura N-95 Masks, surgical masks and particulate masks at inflated prices during the height of the Covid pandemic in early 2020.

Christopher Casamento was the registered owner of Steel City Motor Toys. Casamento, admitted to stealing PPE from his former employer, the University of Pittsburgh while serving as the Director of Emergency Management during the Covid pandemic from February 28, 2020, to March 22, 2020. Masks were shipped to buyers in states outside of Pennsylvania, earning Casamento approximately $18,783.50. Casamento was terminated by University of Pittsburgh officials in July 2020. (Source)

Former University Professor To Plead Guilty To $1.1 Million+ Wire Fraud Scheme Involving Foreign Students And Visiting Professors - February 11, 2022

Beginning in approximately April 2016 and continuing through at least November 2020, Yue Liu, who was an engineering professor at the University of Wisconsin-Milwaukee (UWM).

Liu devised and executed a scheme to obtain money, through materially false promises and representations, from foreign students who were accepted into graduate programs at UWM. Liu promised foreign students that they would be part of a program run by an entity he controlled, which would pay expenses associated with their studies at UWM, including tuition and other costs. In reality, there was no such program affiliated with UWM, and UWM waived the students' tuition because they were research assistants. Liu emailed letters to students in which he made false representations about the program, and he wrote those letters using a fictitious name he invented and using what appeared to be a UWM logo.

Liu fraudulently obtained more than $1.1 million from foreign students and visiting professors. Liu did not use the money from the students to pay their tuition and other expenses. Instead, he used a portion of the money he received for personal purposes, including to fund investment accounts and to pay credit card expenses. Liu also attempted to conceal the scheme by creating a fraudulent research agreement between UWM and a fictitious entity purportedly based in China and using a portion of the money to fund this agreement.

Liu used the money for personal purposes to fund investment accounts and pay credit card expenses. (Source)

Former County Clerk Pleads Guilty To $1.5 Million+ Wire Fraud Scheme For Personal Use - February 22, 2022

A former County Clerk, Jacob Holliday pleaded guilty to taking more than $1.5 million in county money for his personal use.

In June 2020, Craighead County officials reported that a theft had occurred from the Craighead County Clerk's office. The bank that managed the Clerk's office account had flagged suspicious activity, and auditors concluded that approximately $1,579,057.03 was missing and had been moved to Holliday's personal banking accounts. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

Former New York Police Department Union Head Charged In $1 Million+ Fraud Case / Used Funds To Pay For Clothing, Jewelry, Home Appliances, Relative's College Tuition - February 23, 2022

Edward Mullins is the former president of the New York City Police Union.

He has been charged with defrauding the union of hundreds of thousands of dollars by filing false and inflated expense reports for bills that were purportedly for union business, but in fact were not. Mullins submitted the expenses without receipts to the union's treasurer, who approved the reimbursements.

Mullins sought reimbursement for hundreds of high-end meals, clothing, jewelry, home appliances and a relative's college tuition. Mullins was reimbursed by the union over a recent four-year period for $1 Million+ in expenses, the majority of which was fraudulently obtained.

Mullins had also recently been found guilty of two departmental infractions and was fined $32,000 for violating rules governing the use of social media. In one message Mr. Mullins had posted on Twitter, he made public an unredacted police report involving then-Mayor Bill de Blasio's daughter, Chiara. In other messages, Mr. Mullins used vulgar language to denigrate city officials. (Source)

2 Fire / EMS Employees Arrested On Charges Alleging $20,000 Bribery Conspiracy - February 10, 2022
2 District of Columbia Fire and Emergency Medical Services Department (FEMS) employees were arrested on conspiracy and bribery charges for allegedly accepting payments from a District of Columbia contractor in exchange for directing purchase agreements and orders to the contractor and then falsely certifying that goods that FEMS had paid for had been delivered.

Louis Mitchell, a FEMS warehouse supply technician, and Charity Keys, a FEMS contract administrator, accepted bribes over the course of several years—including a bribe of $20,000 each—from the owner of a Maryland limited liability company contractually obligated to provide various goods to FEMS and other District of Columbia agencies. In exchange, Mitchell and Keys allegedly directed purchase agreements and purchase orders to the company and confirmed delivery of and payment for goods that the company did not deliver. (Source)

Former Ambulance Service Treasurer Pleads Guilty To Embezzling $136,000+ To Fund His Flower Shop Business - February 11, 2022
Edward Stevenson was employed as the Administrative Director, and also as served as the Treasurer of Brownsville Ambulance Service, Inc. (BAS), located in Brownsville, Pennsylvania.

From January 17, 2013 through March 22, 2017, Stevenson without authorization issued 132 checks totaling $136,140 from BAS's checking accounts at First National Bank and PNC Bank. He made the checks payable to himself, to cash, and to his personal business, Lunden's Flower Shop. Stevenson deposited the checks in his personal bank account or one of two bank accounts he maintained on behalf of Lunden's Flower Shop, all of which were issued in excess of his wages and for his personal benefit. At the time of the offense, BAS was a not-for-profit business that annually received $10,000 or more in federal benefits through the Medicare and Medicaid programs. (Source)

Former Sheriff's Office Employee Allegedly Received $30,000+ In Unemployment Benefits While Still Being Employed - February 8, 2022
Dawn Hood is a former employee of the Baxter County Sheriff's Office. Hood was employed by the sheriff's office as a secretary from 2014 to 2021.

The criminal investigation was initiated after Baxter County Government was notified Hood had allegedly received unemployment benefits charged against the county.

At the time Hood applied for and received the unemployment benefits, she was employed full-time by the Baxter County Sheriff's Office and had sustained no loss of wages or income from the county during the period in question.

Arkansas Workforce Services notified the Baxter County Human Resources Office that from the first quarter of 2020 through May 2021, $30,762 in unemployment benefits had been paid to Hood. (Source)

Police Officer Arrested For Cocaine Distribution Of 56 Grams While On Duty - February 24, 2022
Keven Rodriguez, a Field Operations Division Officer with the Raleigh Police Department, distributed 56 grams of cocaine while on duty in his patrol car.

The complaint alleges that the investigation began when members of the Raleigh Police Department and the Drug Enforcement Administration received information that Rodriguez was distributing controlled substances in the Raleigh area, and that Rodriguez was a police officer.

The complaint also alleges that a confidential source arranged to meet with Rodriguez on January 24, 2022. Rodriguez drove to the meeting location in his marked Raleigh Police Department patrol car and was carrying his duty firearm. The source met with Rodriguez and gave Rodriguez $2,600 in cash. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Nun Who Embezzled $835,000+ Of Tuition Money From Catholic Elementary School Over 10 Years Sentenced To Prison / Use Money For Gambling & Personal Expenses - February 7, 2022

For a period of 10 years ending in September 2018, Mary Kreuper embezzled money from St. James Catholic School. As principal, a position she held for 28 years, Kreuper was responsible for the money the school received to pay for tuition and fees, as well as for charitable donations. Kreuper controlled accounts at a credit union, including a savings account for the school and one established to pay the living expenses of the nuns employed by the school.

Kreuper falsified monthly and annual reports to the school administration to cover up her fraudulent conduct. She lulled St. James School and the Administration into believing that the school's finances were being properly accounted for and its financial assets properly safeguarded. This in turn, allowed Kreuper to maintain her access and control of the school's finances and accounts and, thus, continue operating the fraudulent scheme. Kreuper also directed St. James School employees to alter and destroy financial records during a school audit.

The total losses Kreuper caused to St. James Catholic School were $835,339. She used the money to pay for personal expenses, including gambling trips. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees To Steal Technology - February 7, 2022

Motorola Solutions developed the Digital Mobile Radio (DMR) technology through years of research and design. Motorola Solutions marketed and sold the radios, which are sometimes referred to as "walkie-talkies," in the United States and elsewhere.

PRC based Hytera Communications Corp. LTD recruited and hired Motorola Solutions employees and directed them to take proprietary and trade secret information from Motorola without authorization. While still employed at Motorola, some of the employees allegedly accessed the trade secret information from Motorola's internal database and sent multiple emails describing their intentions to use the technology at Hytera.

From 2007 to 2020, Hytera and the recruited employees used Motorola's proprietary and trade secret information to accelerate the development of Hytera's DMR products, train Hytera employees, and market and sell Hytera's DMR products throughout the world, the indictment states. Hytera paid the recruited employees higher salaries and benefits than what they received at Motorola. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Swiss Banker Charged With Making Fraudulent Deals Also Tells Court That $200,00+ Strip Club Visits Were Business Related - January 25, 2022

A former top Swiss banker charged with making millions of dollars through fraudulent deals, stated that a near $217,675 expenses bill for strip club visits was largely business-related.

Pierin Vincenz, once a Banker Of The Year, also told a Zurich court that the dinner with a woman he met on dating app Tinder, was justified because he was considering her for a real estate job and a trip to Australia was made to examine the country's ATMs.

Most of the charges facing Vincenz in Switzerland's highest profile corporate crimes trial in decades relate to allegations of illegal trades while he was chief executive of unlisted cooperative lender Raiffeisen Switzerland.

Other expense included nearly 4,000 francs for the repair of a hotel room at the five-star Zurich Park Hyatt, which was damaged during a "massive row" between Vincenz and a strip club dancer he was dating at the time. (Source)

Former Bank Branch Manager (Member Of Criminal Fraud Ring) Pleads Guilty To Tech Support Fraud Scheme That Exploited The Elderly - February 2, 2022

From approximately November 2017 through June 2019, Ariful Haque was a member of a criminal fraud ring based in the United States and India that committed a technical support fraud scheme that exploited score of victims located across the United States and Canada, including in the Southern District of New York. The fraud ring's primary objective was to trick victims into believing that their computers were infected with malware, in order to deceive them into paying hundreds or thousands of dollars for phony computer repair services.

The scheme generally worked as follows. First, the Fraud Ring caused pop-up windows to appear on victims' computers. The pop-up windows claimed, falsely, that a virus had infected the victim's computer. The pop-up window directed the victim to call a particular telephone number to obtain technical support. In at least some instances, the pop-up window threatened victims that, if they restarted or shut down their computer, it could "cause serious damage to the system," including "complete data loss." In an attempt to give the false appearance of legitimacy, in some instances the pop-up window included, without authorization, the corporate logo of a well-known, legitimate technology company. In fact, no virus had infected victims' computers, and the technical support phone numbers were not associated with the legitimate technology company. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE & STAFF

10 People, Including 2 Medical Doctors Charged In A $300 Million Healthcare Fraud / Kickback Scheme - February 10, 2022

According to the indictment, the founders of several lab companies, including Unified Laboratory Services, Spectrum Diagnostic Laboratory, and Reliable Labs LLC, allegedly paid kickbacks to induce medical professionals to order medically unnecessary lab tests, which they then billed to Medicare and other federal healthcare programs.

The labs, through marketers, allegedly paid doctors hundreds of thousands of dollars for "advisory services" which were never performed in return for lab test referrals. They also allegedly paid portions of the doctors' staff's salaries and a portion of their office leases, contingent on the number of lab tests they referred each month. In some instances, lab marketers even made direct payments to the provider's spouse.

When the labs threatened one provider that payments would cease if he didn't refer more tests, he immediately increased his lab referrals, averaging approximately 20 to 30 referrals per day. (Source)

Nursing Home Accounts Receivable Manager Accused Of Stealing $100,000 From Elderly Bank Accounts After She Was Asked To Resign - February 20, 2022

Patrica Myler worked as an Accounts Receivable Manager at Villa St. Francis in Olathe, Kansas. She was asked to resign from her position on Dec. 9, 2020 due to poor performance.

In the weeks after she was asked to resign, more than $40,000 had been transferred from a resident living at Villa St. Francis into Myler's bank account.

When Villa St. Francis conducted an audit, it was determined that Myler made dozens of transfers and ATM withdrawals from the accounts of at least seven residents living at the facility. They also showed the transfers began more than two years ago.

Court documents show residents and their families saying Myler offered to help set up automatic payments to cover their expenses. She allegedly told at least some of the families that the easiest way to set up a scheduled payment was to provide her with an ATM card and PIN.

Myler lived paycheck to paycheck in the six months before she was hired at Villa St. Francis. When she started working, her monthly paychecks averaged $3,233.10, but her spending was three to six times more than she made each month. The affidavit also shows that the total amount of money Myler spent using her personal account in 2020 was more than $175,000. That was more than four times her reported salary of $40,727.71. (Source)

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD/ BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING

Former Bookkeeper Convicted For Embezzling $700,000 From 2 Employers / $950,000 From Another Employer - February 22, 2022

Kimberly Janovec was convicted on 24 counts of fraud, aggravated identity theft, and tax crimes. Notably, Peterson-Janovec has a prior federal fraud conviction from 1998, when she embezzled more than $950,000 from another former employer.

In 2014, Kimberly Janovec became the Director of Operations for MI5, Inc., a Denny's franchisee that owned and operated eight Denny's franchises in Minnesota and Wisconsin. In this role, Peterson-Janovec had extensive managerial oversight for all eight restaurants, including payroll, cash deposits, vendor and contractor billing, marketing, and coordinating reimbursements from Denny's Corporate.

From April 2014 through July 2019, Peterson-Janovec used her position to embezzle funds from MI5 and Denny's Corporate by generating and submitting false requests for vendor payments and then diverting those payments for her own use and benefit. Peterson-Janovec also manipulated the company's payroll system to issue herself unauthorized compensation using the names of employees who no longer worked for the company. As part of the scheme, Peterson-Janovec falsified records, created fake email accounts, and generated fake email traffic in which she impersonated employees of various purported vendors. In total, Peterson-Janovec received approximately $336,000 in bogus vendor payments and approximately $20,000 in fraudulently issued payroll submissions using the identities of other people.

In July 2019, MI5, Inc., discovered aspects of Janovec's fraud and terminated her employment. After her termination, in early 2020, Janovec lied about her work experience to get another bookkeeping job with a family owned construction company. Janovec started as its bookkeeper, and eventually was promoted to its general manager. Janovec used her access to the company's QuickBooks, to issue herself numerous payments, and she did so in a manner that made the payments appear as if they were going to the company's vendors. This netted -Janovec another $350,000 in as little at 18 months.

In total, Janovec stole more than $700,000 from her employers, which she used to finance her lifestyle and hobbies, including a substantial down payment on her personal residence. (Source)

Former Hewlett-Packard Employee Charged With $4.8 Million Credit Card Fraud Scheme To Purchase Tesla & 200 Luxury Items - February 14, 2022

Federal prosecutors have charged a former HP Inc. employee (Shelbee Szeto) with stealing roughly $4.8 million from company credit cards from 2018 to 2021, money she allegedly used to buy hundreds of designer bags, jewelry and a Tesla.

The charging records allege that she stole millions by simply making personal charges to company credit cards, and linking HP credit cards to her personal bank account with First Republic.

When first confronted, Szeto claimed to have made millions in legitimate income in less than a year, and filed false tax returns to cover her tracks. When a First Republic Bank employee questioned the source of the fraudulent funds that Szeto stole from HP, Szeto falsely represented to the employee that the deposits were legitimate business income from her work as a consultant and that she had received approximately $3.6 million in legitimate business income between approximately May 2020 and April 2021.

Mentioned in the charging records are approximately 200 luxury items Szeto allegedly bought, including crocodile handbags, Chanel purses, Rolex watches, a 2020 Tesla sedan, a Louis Vuitton teddy bear, a Cartier diamond ring, and a half-dozen gold necklaces. Federal prosecutors have moved to seize the items, alleging they're the spoils of the fraud scheme. (Source)

Former Director Of Accounting And Human Resources Charged With Embezzling $500,000+ For Personal Expenses (Beauty Treatments, Jewelry, Clothing, Corvette, Utility Bills) - February 9, 2022

In October 2019, Susan Rivera was hired as the Director of Accounting and Human Resources at the victim company, a family owned kitchen design and remodeling business.

Starting in November 2019, Rivera made hundreds of unauthorized charges in a total amount exceeding $175,000 to the victim company's credit cards for personal expenses, including jewelry, beauty treatments, laser treatments, travel, pets, cosmetic surgery, clothing and cars, including a partial payment on a $100,000 Corvette.

Rivera also caused the victim company's payroll company to make unauthorized payments in a net amount of more than $370,000 to a fake vendor that she created to receive the money.

Rivera made unauthorized transfers from the victim company's bank account in an amount exceeding $2,900 to pay her personal utility bills. To get restrictions on the use of the victim company's credit cards removed, Rivera posed as an owner of the victim company in telephone calls with the company's credit card company. Rivera also sent the credit card company photographs of the owner's driver's license to cause credit card company personnel to believe she was the owner. Rivera embezzled more than $550,000 from her employer. (Source)

Former Verizon Network Engineer Charged With Committing $1 Million In Fraud / Used Funds To Purchase 2 Boats & Motorcycle - February 2, 2022

Jeremie Elkins was charged for allegedly causing approximately $1 million in fraud while employed as a network engineer at Verizon, Inc.

From July to October 2020, Elkins used his company-issued credit card to pay for personal expenses like hotels / resorts, restaurants, bars, pawn shops and auction houses.

Elkins also allegedly used an old Verizon work order number to place multiple fraudulent orders with vendor W.W. Grainger, Inc. Grainger provides tools and equipment for Verizon service vans. It is alleged Elkins placed 46 unauthorized orders to Grainger and personally picked up the majority of the equipment, which totaled approximately $936,000. He allegedly used the illicit proceeds to purchase two boats and a motorcycle.

Elkins placed an additional 20 unauthorized orders to Grainger, for items totaling nearly $954,000, but never obtained the equipment. (Source)

Accounts Payable Clerk Pleads Guilty To Transferring $300,000 To Personal Bank Account To Pay Bills - January 31, 2022

Grant Devillez admitted that from at least February 2016 through July 2018, he engaged in a scheme to defraud Décor Craft, Inc., of approximately $302,000, by misappropriating funds from the business' bank accounts and transferring those funds to his own personal bank accounts, to his creditors to pay personal bills, and to the bank account of another person in Massachusetts.

Mr. Devillez admitted that he was given access to the Décor Craft, Inc. bank account to make authorized payments to vendors. He admitted that, instead of making those payments, he would either make a partial payment to the vendors, or no payment at all, and would transfer the remaining funds for his own use. Afterwards, he altered company records to reflect that full payment had been made to vendors. (Source)

Condominium Property Manager Charged With Stealing Cash To Use At Casino - January 31, 2022

Cheryl Sullivan, a real estate broker, tax preparer, property manager, and the chairperson of the Board of Tax Assessors for the Town of Dedham, Massachusetts (MA), was arrested by FBI agents.

Sullivan, acting in the capacity as a Property Manager for the River Island Condominium Association, devised a scheme to access Association funds for her own personal use. It is alleged that beginning as early as February 2019, Sullivan used a debit card attached to the association's checking account to withdraw cash for her own use from ATMs located at the casino in Plainville, MA. (Source)

Former Office Manager Sentenced To Prison For Embezzling Approximately $725,000 - February 3, 2022

During a seven-year period while Michelle Clabough was employed as an Office Manager, she forged more than 250 checks and embezzled $725,770 from her employer. (Source)

Former Senior Accounting Manager Charged With Stealing $3 Million From Employer For Use On Personal Expenses & Family - February 4, 2022

From 2011 to 2018, Jennifer Vandever worked as a supervisor in her company's accounting department.

Vandever embezzled from the company by charging significant amounts of personal expenses for herself and her family on the company's various corporate credit cards. The scheme totaled $3 million. (Source)

Former Employee Of Mechanical Contractor Admits To Construction Project Fraud Scheme / Used Funds For Children's College Tuition, Airline Tickets, Hotels, Rent - February 14, 2022

William Sacco was a project manager for a Massachusetts-based mechanical contractor.

From June 2014 to December 2017, Sacco conspired to defraud his employer and the owners of certain projects he managed by inflating change orders on the projects. As part of the conspiracy, a co-conspirator subcontractor made more than $200,000 in payments to Sacco and also for Sacco's benefit, including payments for Sacco's children's college tuition, a graduation party, a Mac laptop, airline tickets, hotels and Sacco's rent. Sacco and the co-conspirator submitted inflated change orders to Sacco's employer to offset some of the costs of the payments the co-conspirator made to Sacco. (Source)

Former Chief Financial Officer Of The Boston Grand Prix Sentenced To Prison For $2 Million Fraud & Tax Schemes / Used Money For 3 Carat Diamond Ring, Private School Tuition, Luxury Hotel Visits - February 15, 2022

John Casey became the CFO of the Boston Grand Prix in January 2015.

Casey was sentenced to prison in connection with multiple schemes to defraud equipment and small business financing companies as well as the Small Business Administration and the Internal Revenue Service.

Casey used fraudulently obtained pandemic grant funds to pay for three-carat diamond ring, online dating membership, private school tuition and luxury hotel stays. (Source)

Former Employee Charged With Defrauding Employer Of $549,000+ - February 18, 2022

Michael Goll was the New Orleans branch manager of a company which provides material handling equipment to businesses.

From January 2013 through September 2017, Goll defrauded his company of approximately $549,667.39. Goll is alleged to have executed the scheme by sending his company false invoices from shell companies that he had created, when in fact the work was either done by th company's own employees or the work was not done at all. (Source)

Office Secretary For Auto Body Shop Sentenced To Prison For $220,000+ Fraud Scheme - February 18, 2022

Idalee Johnston while working as Office Secretary for a auto body business, devised a scheme to fraudulently obtain the proceeds of nearly 200 checks provided to customers by their insurance companies to pay for vehicle repairs.

Beginning in 2016, Johnston used two methods to obtain these funds: in some cases, she would not have customers sign direct payment forms that would have caused their insurance payments to be made directly to the auto body shop for repair work; in other cases, where customers did sign payment forms, she would not forward them to the insurance companies. As a result of her actions, insurance checks to pay for repairs were sent directly to customers who, in turn, at Johnston's direction, provided the checks to her as a representative of the business.

Johnston admitted to the court that she deposited some of the checks into her bank account. In other instances, stolen checks were provided to family members to be deposited into their bank accounts, and later, at her direction, these family members provided her with most of the funds.

The scheme continued for two years, resulting in a loss to the auto body business of more than $220,000. (Source)

Former Director Of Finance For Music Society Admits To Embezzling $650,000 Over 10 Years To Pay Mortgage, Credit Card, Etc. - February 23, 2022

Chris Benavides pleaded guilty to wire fraud, admitting that while employed as the Director Of Finance for the La Jolla Music Society, he embezzled more than $650,000 over a 10-year period.

Benavides admitted he abused his access to the company's accounting software and issued unauthorized checks to himself.

Benavides used the La Jolla Music Society's money to pay his mortgage, credit cards, and other personal expenses. He then concealed the payments by manipulating the company's accounting records to make it appear that they were legitimate business expenses. (Source)

Former County Director Of Utilities Pleads Guilty To $30,000+ Wire Fraud Conspiracy For Accepting Bribes - February 23, 2022

From 2012 to 2018, Barry Edwards and an unnamed individual identified in court documents as the Contractor, devised a bribery and kickback scheme involving the Catawba County Government contracts.

Edwards admitted as Director of Utilities and Engineering, had the authority to review and award on behalf of the county government contracts to private businesses for engineering and consulting activities related to the County's landfill, solid waste and natural gas projects. Edwards admitted to awarding contracts to three businesses, all while receiving gifts and other things of value that influenced his decisions, including expensive meals, tickets to sporting events, and wine-tasting tours, totaling more than $30,000. (Source)

Former Executive Director Of Miss Florida Scholarship Program Charged With Fraud / Use Funds For Personal Expenses

Mary Wickersham served as the Executive Director of the Miss Florida Scholarship Program, Inc., a not-for-profit organization that raises money to provide scholarships to young women through pageants. Wickersham had access to the pageant program's financial information, as well as its sponsors and donors.

While serving as the Executive Director, and without notifying the Board of Directors of the Miss Florida Scholarship Program, Mary Wickersham opened a company under the name "Miss Florida," which she then used to open a business account at Bank of America. Wickersham solicited donations and contributions on behalf of the Miss Florida Scholarship Program from sponsors and donors.

Rather than depositing donations into the organization's legitimate bank account, Wickersham altered donor checks and deposited money into her "Miss Florida" account at Bank of America. Wickersham used the money to pay for her personal expenses, including utilities, shopping, home goods, maid cleaning service, online dating fees, and dining out, it is alleged. (Source)

Former National Fraternity Treasurer Sentenced To Prison For Embezzling $2.9 Million - February 22, 2022

Curtis Anderson served as the Director of Finance for the fraternity. He was authorized to make deposits into the organization's bank accounts but was not allowed to sign checks.

Beginning as early as 2012, the defendant wrote numerous large checks to himself without permission using the signature stamps of authorized signatories, and withdrew cash from the fraternity's bank accounts without permission. He also wrote checks payable to several other individuals who worked for the fraternity, without their knowledge, and then forged their endorsements, cashed the checks, and pocketed the money. In total, the defendant embezzled over $2.94 million from the fraternity over a six-and-a-half-year period. (Source)

Former Office Manager Sentenced To Prison $39,000+ Bank Fraud - February 25, 2022

Melissa Castellanos, worked as a financial specialist and office Manager at Aspire Human Services in Idaho.

From at least July 2015 through August 2017, Castellanos executed a scheme to defraud that included preparing and cashing checks for fraudulent purchases on residents' accounts.

Castellanos wrote inaccurate descriptions in the memo lines of the checks to help conceal her actions. After preparing and signing the checks for fraudulent purchases, Castellanos cashed the checks. Castellanos went to the bank alone, instead of brining the residents whose money she was taking. Castellanos kept the cash and did not provide it to the residents or use it to purchase the goods identified in the memo lines.

Castellanos must pay $39,950.89 in restitution. (Source)

Former Supermarket Cashier Pleads Guilty To $87,000+ Fraud Scheme - February 25, 2022

Wanda Goode, was a cashier at a supermarket located that sold Visa prepaid debit cards.

From April 2019 to September 2019, Goode fraudulently activated numerous prepaid cards for her own personal use. During the scheme, Goode made more than $87,000 in fraudulent purchases or payments with the prepaid cards. (Source)

WORKPLACE VIOLENCE

Former Hospital Nurse Beats & Sets Another Employee On Fire - February 9, 2022

A New Jersey man accused of setting fire to and assaulting a fellow hospital employee was found to have died of a self-inflicted gunshot wound hours into the manhunt for his arrest.

Nicholas Pagano, was wanted on charges of attempted murder, aggravated arson, aggravated assault and unlawful possession of a weapon for allegedly setting a female coworker on fire inside Hackensack University Medical Center.

Pagano, who was a nurse, allegedly attacked and burned the 54-year-old woman inside a hospital break room. He used a wrench to beat the woman during the assault.

Meanwhile, the victim was treated at the hospital for cuts to her head and third-degree burns covering her face, hands and upper body. She was later transported to a different hospital, but is expected to survive. (Source)

PREVIOUS INSIDER THREAT INCIDENT REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data (2021)

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021. Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files. After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

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

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

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

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

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

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

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

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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**3,400+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

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

Incident Posting Notifications

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

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

https://twitter.com/InsiderThreatDG

Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

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

The NITSIG has created a Linked Group for individuals that interested in sharing and gaining in-depth knowledge regarding ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in ITM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **875+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over 10+ years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

Our training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org