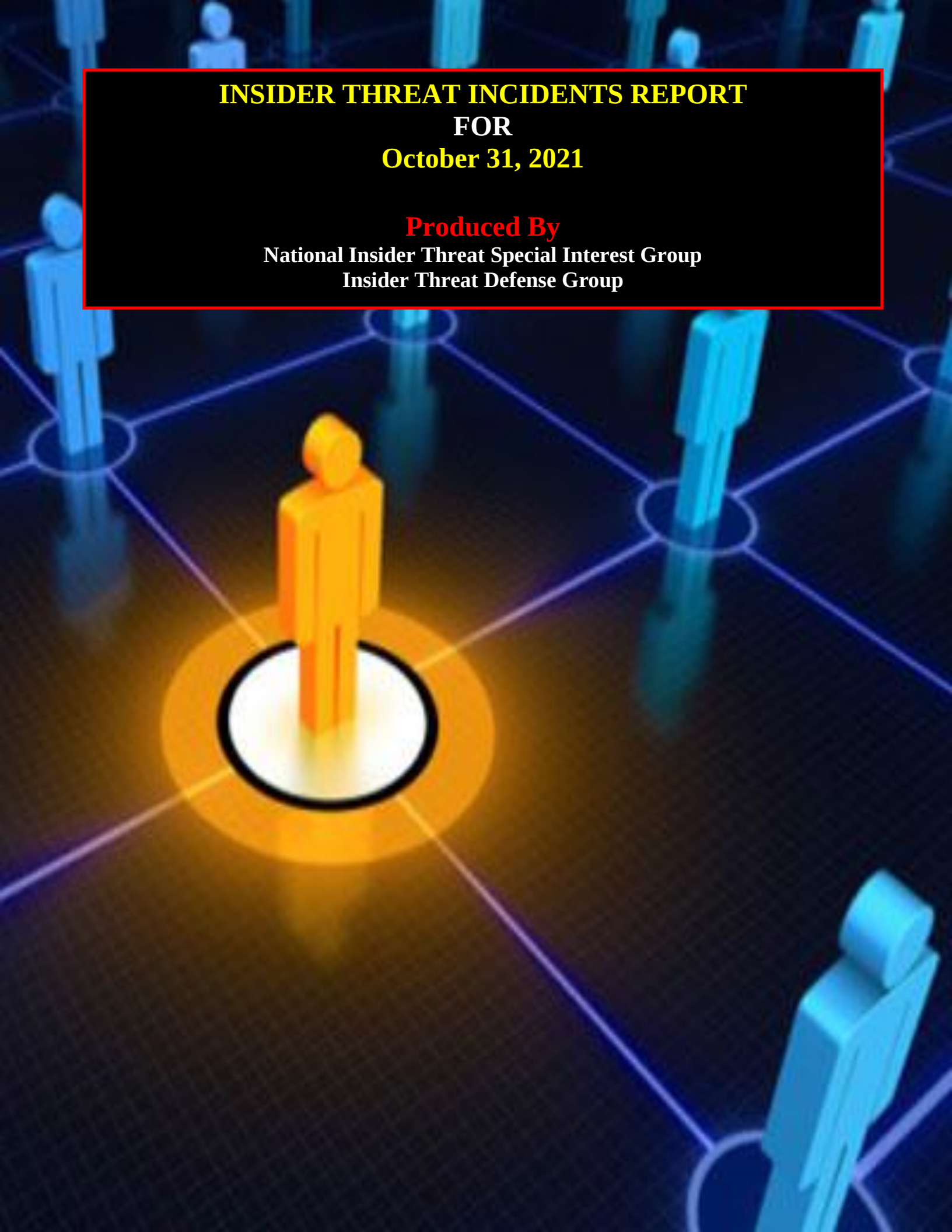

INSIDER THREAT INCIDENTS REPORT
FOR
October 31, 2021

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 **3,100** 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 22 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 OCTOBER 2021

U.S. GOVERNMENT

Former Operations Supervisor At Social Security Administration Sentenced To Prison For $760,00 Wire Fraud / Identity Theft Scheme - October 4, 2021

Stephanie Chavis was an Operations Supervisor at the Social Security Administration (SSA).

Chavis had access to SSA beneficiary accounts and associated personal identifying information (PII). Between approximately August 2010 and April 2018, Chavis caused over $760,000 in SSI benefits to be electronically deposited into nine different bank accounts held in her name, and in the names of various family members, by making false and fraudulent representations to fellow SSA employees, including claims representatives and other supervisors. The investigation established that Chavis used her government-issued PIN number to query the accounts of approximately 62 program beneficiaries and used their PII to generate the fraudulent payment requests. The beneficiaries targeted by Chavis included incarcerated individuals who were not entitled to payments, individuals who had been suspended or terminated from the SSI program, and beneficiaries who were legitimately owed SSI funds.

To circumvent SSA policy requirements, Chavis provided the beneficiary PII and account information for deposit purposes to unsuspecting claims representatives and asked them to create approximately 100 fraudulent payment requests. After the requests were created, Chavis either approved them herself or asked other SSA employees to process the approvals. Thereafter, the stolen funds were deposited into the bank accounts under Chavis's control. (Source)

Former IRS Employee Charged With Tax Fraud - October 20, 2021

Wayne Garvin allegedly filed individual income tax returns for the years 2012 through 2016 on which he claimed fraudulent deductions and expenses, including charitable contribution deductions and expenses associated with rental properties that he owned for some years. For the year 2013, Garvin also allegedly claimed he had expenses associated with service in the U.S. Army Reserves even though he did not perform any reservist duty that year. At the time Garvin filed his false tax returns, he was employed as a Supervisory Associate Advocate with the IRS's Taxpayer Advocate Service in Philadelphia.

After the IRS began an audit of Garvin's 2013 and 2014 tax returns, Garvin submitted fraudulent documents to the IRS revenue agent conducting the audit. Among other fraudulent documents, Garvin allegedly created receipts from a church, invoices from a contractor and a letter from the Department of the Army in an attempt to convince the IRS he was entitled to claim the deductions and expenses on his returns. Garvin allegedly submitted the fraudulent documents to the IRS to prevent the IRS from assessing additional taxes against him for 2013 and 2014. Finally, the indictment alleges that after the IRS notified Garvin that he was under criminal investigation for filing false tax returns, Garvin provided the same fraudulent documents to IRS Criminal Investigation that Garvin previously provided to the IRS revenue agent. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Navy Nuclear Engineer & Spouse Charged With Espionage - October 7, 2021

Jonathan and Diana Toebbe, both of Annapolis, Maryland, were arrested by the Federal Bureau of Investigation (FBI) and the Naval Criminal Investigative Service (NCIS) on Saturday, October 9, 2021.

Jonathan Toebbe is an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program, also known as Naval Reactors. 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.

On April 1, 2020, 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. 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.

On June 8, 2021, the undercover agent sent $10,000 in cryptocurrency to Jonathan Toebbe as "good faith" payment. Shortly afterwards, on June 26, 2021, Jonathan and Diana Toebbe traveled to a location in West Virginia. There, with Diana Toebbe acting as a lookout, Jonathan Toebbe placed an SD card concealed within half a peanut butter sandwich at a pre-arranged "dead drop" location. After retrieving the SD card, the undercover agent sent Jonathan Toebbe a $20,000 cryptocurrency payment. In return, Jonathan Toebbe emailed the undercover agent a decryption key for the SD Card. A review of the SD card revealed that it contained Restricted Data related to submarine nuclear reactors. On August 28, 2021, Jonathan Toebbe made another "dead drop" of an SD card in eastern Virginia, this time concealing the card in a chewing gum package. After making a payment to Toebbe of $70,000 in cryptocurrency, the FBI received a decryption key for the card. It, too, contained Restricted Data related to submarine nuclear reactors. The FBI arrested Jonathan and Diana Toebbe on October 9, after he placed yet another SD card at a pre-arranged "dead drop" at a second location in West Virginia. (Source)

Former Veteran Affairs Supervisor Sentenced To Prison For $1 Million+ Of Theft Of Government Property And Fraud - October 14, 2021

According to court documents, from October of 2010, through January of 2019, William Precht worked as an Inventory Management Specialist and later as a Supervisory Management and Program Analyst at the Cleveland VA Medical Center. Through his positions at the VA, Precht could order medical supplies, purchase capital equipment and monitor requests for equipment purchases.

Using his position and his VA employee log-in information, Precht registered a purported vendor (Vendor-1) as a Small Disadvantaged Business and Veteran-Owned Small Business in the VA vendor system. Beginning in October of 2010, Precht used his VA purchase card and other employee cards to purchase purported medical supplies from Vendor-1, a company he controlled, in the amount of approximately $1,066,348.

In addition, from May of 2015 through January of 2019, Precht conspired with Robert A. Vitale, a medical sales representative for multiple companies that conducted business with the Cleveland VA, to devise a scheme in which Precht would receive kickbacks and other items of value, in exchange for steering VA business and other monetary awards to Vitale.

In order to conceal his schemes, Precht provided false and misleading information to VA employees about reasons for ordering medical supplies and falsified patient records. As a result, the Cleveland VA suffered a loss of $193,042.66.

Robert. A. Vitale pleaded guilty on October 13, 2021 for his role in the scheme. (Source)

Former Army Contractor Sentenced To Prison For $1.5 Million Fraud Scheme With 4 Conspirators Targeting 3,300+ U.S. Service Members & Veterans - October 1. 2021

Fredrick Brown was sentenced for one count of conspiracy to commit wire fraud and one count of conspiracy to commit money laundering following Brown's guilty plea on Oct. 29, 2019.

Brown conspired with four other individuals to steal money belonging to military members, and military dependents and civilians employed by the U.S. Department of Defense. The scheme targeted over 3,300 members of the U.S. military community resulting in $1.5 million in losses.

Brown, a former civilian medical records technician and administrator with the U.S. Army at the 65th Medical Brigade, Yongsan Garrison, South Korea, admitted that between July 2014 and September 2015, he stole the personal identifying information (PII) of thousands of military members, including names, Social Security numbers, military ID numbers, dates of birth and contact information.

Brown also admitted to capturing the PII by taking digital photographs of his computer screen while he was logged into a military electronic health records database and, subsequently, providing the stolen data to Philippines-based co-defendant Robert Wayne Boling Jr. Boling and others, who used the information to access DOD and Veterans Affairs benefits sites and steal millions of dollars.(Source)

United States Naval Intelligence Software Engineer Pleads Guilty To Conspiracy To Distribute Steroids Over 10 Years - October 27, 2021

From 2013 to April 2021, Justin Best operated an illegal steroid manufacturing business from his Laurel, Maryland residence and conspired with others to distribute and possess with the intent to distribute, home manufactured steroids throughout the United States.

Llaw enforcement executed a search warrant at Best's Laurel, Maryland residence. Officers located and seized 8,500 units of controlled substances used in manufacturing steroids, including two 2,000-milliliter jars of testosterone cypionate, 198 pills of oxandrolone, 114 pills of stanozolol, 61 pills of oxymetholone, nine 10-milliliter vials of testosterone enanthate, one 10-milliliter vial of testosterone phenylpropionate, syringes, and packaging and mailing materials.

In addition to precious metals, collectable coins, and $6,127 in cash, officers recovered approximately 167 firearms consisting of 120 handguns, 39 rifles, seven shotguns, and 25 silencers. Officers also seized hundreds of thousands of rounds of ammunition, as well as 277 firearm magazines and 18 sets of firearm accessories from Best's garage. Best agreed that the seized firearms, silencers, ammunition, magazines and firearm accessories were purchased with proceeds of his manufacturing and distribution of controlled substances. (Source)

Former Air War College Professor Pleads Guilty To Making False Statements About Relationship With Government Official In China - October 25, 2021

Xiaoming Zhang a naturalized citizen of Chinese descent living in Montgomery, Alabama, began working as an Air War College (AWC) professor in July 2003. During his tenure at the AWC, Zhang would travel to China on a regular basis for work-related purposes, research and to visit family living there.

Beginning sometime in 2012, Zhang developed a relationship with a known foreign official working with the Shanghai Municipal Government. Records indicate that Zhang met with the official in person on approximately six occasions and exchanged approximately 40 emails with him from December 2012 to January 2017. At some point during this period, Zhang became aware that the official was using, or attempting to use, their relationship to gain access to sensitive information in Zhang's possession, as well as to make contact with other potentially valuable individuals.

Zhang failed to report the relationship with the foreign official even after he came to understand that the official was attempting to gather sensitive information from Zhang. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

Two Correctional Officers Plead Guilty To Racketeering Conspiracy, Admit To Smuggling Contraband Into Federal Pretrial Detention Facility In Exchange for Bribes - October 19, 2021

As detailed in their plea agreements, Darren Parker and Talaia Youngblood, along with other employees, detainees and associates of Chesapeake Detention Facility (CDF), in Baltimore, knowingly participated in a conspiracy to smuggle contraband into CDF, including narcotics, cell phones, and tobacco. Parker and Youngblood admitted that they abused their positions of trust as sworn officers of DPSCS by engaging in illegal activities to enrich themselves. (Source)

Three Former NYPD Police Officers Plead Guilty To Accident Tow Truck Response Bribery Scheme - October 7, 2021

Robert Hassett, a former New York City Police Department (NYPD) Officer, pleaded guilty to conspiring to participate in a scheme to sell the personal information of automobile accident victims in exchange for bribes (Victim Database Scheme- VDBS) . Hassett also admitted that he participated in a scheme to steer vehicles damaged in automobile accidents to a tow truck company in contravention of NYPD's Direct Accident Response Program (DARP) in exchange for bribes. (Two Truck Scheme)

Former NYPD officer Heather Busch pleaded guilty to accepting bribes in connection with her participation in the Tow Truck Scheme. A third defendant, retired NYPD officer Robert Smith, pleaded guilty to accepting bribes in connection with his participation in the Tow Truck Scheme.

At the time that they participated in the Tow Truck Scheme and the VDBS, the Hassett amd Smith were NYPD officers assigned to the 105th Precinct in Queens, New York.

Bbetween 2016 and 2017, Hassett and Smith received thousands of dollars of bribe payments in exchange for referring business to a towing company, contrary to DARP. Smith resumed the corrupt scheme without Hassett in late 2019 and when Smith retired from the NYPD in March 2020, Smith enlisted Busch to take his place in the scheme.

In early 2020, Smith and Hassett also sold the names and contact information of automobile accident victims whose accidents occurred within the confines of the 105th Precinct for thousands of dollars in bribe payments, ostensibly so that the purchaser could resell that personal information to physical therapy businesses and personal injury lawyers who would contact the automobile accident victims as prospective customers. (Source)

3 Current And Former NYPD Officers Charged With Accepting Thousands Of Dollars In Bribes From Tow Truck Company - October 1, 2021

Beginning in approximately May 2020, after James Davneiro and Giancarlo Osma responded as NYPD officers to automobile accidents, they would steer the damaged vehicles to a licensed tow trucking and automobile repair business operated by Michael Perri (Former NYPD officer) , instead of using the NYPD's Directed Accident Response Program, as legally required.

In exchange for steering the removal and repair of damaged vehicles to Perri's business, Perri paid Davneiro and Osma thousands of dollars in cash bribes.

During the relevant period, Davneiro, Osma, and Perri were New York City Police Department (NYPD) officers assigned to the 107th Precinct in Queens. Perri retired from the NYPD in June 2020. (Source)

Former Police Officer Charged With Illegally Obtaining $9,800+ By Falsifying Time Records - October 7, 2021

Jay Cobb is a former police officer with the Village of Alorton Police Department.

Jay Cobb falsified time records for the period of January 2020 through April 2021. He acknowledges that he obtained funds by fraud from May 2018 through April 2021 claiming to be working when he was out of the jurisdiction, usually at his residence in Cahokia, Illinois. He caused a financial loss of approximately $9,815. (Source)

Former Treasurer Of Volunteer Fire Department Charged With $50,000 Of Bank Fraud - October 6, 2021

Between May 2011 and September 2013, Denny Mackey allegedly obtained tens of thousands of dollars from financial institutions by applying for unauthorized loans purportedly to be used for fire department purposes, unbeknownst to the fire department's leadership.

Mackey fraudulently applied for a $75,000 loan purportedly for fire department expenses in August 2013. He falsely represented to the bank that the money would be used to fund the salary of a full-time fire department employee – knowing full well that the volunteer force didn't employ any full-time staff.

Shortly after the bank issued the loan, which he concealed from the fire department, Mackey allegedly withdrew more than $50,000 – some out in cash and the rest by writing fire department checks to a company he controlled. (Source)

Former Boston Police Officer Charged For $16,000+ Overtime Fraud Scheme - October 4, 2021

According to charging documents, from at least January 2015 through February 2019, Thomas Nee submitted false and fraudulent overtime slips for overtime hours that he did not work at the evidence warehouse. As a result, between January 2015 and August 2017, Nee personally collected approximately $16,642 for overtime hours he did not work.

Nee is the 15th Boston Police officer to have been charged in connection with committing overtime fraud at the Boston Police Department's evidence warehouse. Nine of the charged officers have pleaded guilty. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS

State Representative Charged In $600,000 Billing Fraud Scheme For Fake Consulting Services - October 20, 2021

Michael DiMassa has been employed by the City of West Haven, Connecticut for approximately 12 years and has most recently served as the Administrative Assistant to the City Council. He is also currently a Connecticut State Representative. In January 2021, DiMassa and another individual formed Compass Investment Group, LLC. Beginning in February 2021, Compass Investment Group LLC fraudulently billed the City of West Haven and its "COVID-19 Grant Department" for consulting services purportedly provided to the West Haven Health Department that were not performed. From February 2021 through September 2021, the City of West Haven paid Compass Investment Group a total of $636,783.70.

It is further alleged that DiMassa made several large cash withdrawals from the Compass Investment Group LLC bank account, some of which were made shortly before or after he was recorded as having made a large cash "buy-in" of gaming chips at the Mohegan Sun Casino. (Source)

Former City Councilman Sentenced To Prison For $746,000 Fraud Scheme - October 8, 2021

From January of 2010 through October of 2018, Kenneth Johnson (City of Cleveland Councilman) and Garnell Jamison devised a scheme to induce the City of Cleveland to issue reimbursement checks to Johnson for Ward 4 services that were never actually performed. The City issued $1,200 monthly expense reimbursement checks to Johnson totaling approximately $127,200. Each reimbursement check from the city was deposited into Johnson's personal bank account. (Source)

Former City Clerk Sentenced To Prison For $315,000 Fraud Scheme To Pay For Personal Expenses - October 13, 2021

From 2004, Tracey Ray was the City Clerk of Center, Missouri. Beginning in January 2015 and continuing through July 2019, Ray engaged in a scheme to defraud and obtain money from Center, Missouri and its residents in an approximate amount of $315,000, by means of materially false and fraudulent pretenses, representations and promises.

On approximately 30 occasions, Ray used Center bank funds to pay for charges on her personal credit card. Center funds used to pay for personal charges on Ray's GM credit card totaled approximately $206,342.53 and were for such personal expenses as retail vendor charges, entertainment, lodging and travel, hair salons, restaurants and grocery store charges. These personal credit card payments were made either by Ray's issuance of Center bank checks, or by Ray's wire transfer of Center bank funds. On approximately 39 occasions, Ray issued Center bank account checks in the approximate total amount of $62,537.76 to Anthem Blue Cross and Blue Shield to pay for the premiums on a family health insurance policy, as well as on life and disability policies for her and her family members.

As a further part of her scheme, Ray issued five additional Center payroll checks to herself in the total amount of approximately $3,580.00, depositing each of those unauthorized checks into her own personal bank account. On 49 occasions, Ray issued checks on City bank accounts, in the total approximate amount of $35,546.85 to directly pay for the purchases of personal items and services. Ray issued these Center checks to make personal purchases at a number of retailers, such as Kohl's, Lowe's, Walmart, and Hobby Lobby, as well as to pay for her personal residential mortgage and personal insurance policies.

She also issued one or more of these Center checks to her family members, unrelated to the legitimate business and operations of Center. Further, Ray, as Center's City Clerk, received cash payments from Center residents for various city charges, but Ray failed to deposit those cash receipts into the appropriate Center bank account. Instead, Ray used those cash proceeds, in the total amount of approximately $7,407.45 for her own personal use, without the knowledge and authority of Center and its City Council.

In order to conceal her scheme from Center and its Mayor and City Council, Ray falsified the cash balances of one or more Center bank accounts on financial reports she prepared for monthly City Council meetings. Ray also prepared false and incomplete lists of bills to be paid which she submitted for monthly City Council meetings. Further, Ray falsified internal Center financial accounting records to make it appear that the unauthorized checks and wires she issued from Center bank accounts were made to legitimate third party vendors who had purportedly provided actual services or materials to Center. (Source)

Former Georgia Insurance Commissioner Sentenced To Prison For Stealing $2.5 Million+ - August 13, 2021

From January 2012 until Jim Beck was sworn in as Georgia Insurance Commissioner on January 14, 2019, Beck worked as the General Manager of Operations for the Georgia Insurance Commissioner (GUA).

While Beck served as General Manager of GUA, he also maintained controlling financial interests in two businesses known as Creative Consultants and the Gerogia (GA) Christian Coalition. Beginning in 2013, Beck talked four associates—all of whom were either friends or family members--into forming four separate businesses that supposedly supplied necessary services, including residential property inspections and water damage mitigation, to GUA. Then, through an elaborate system of fraudulent invoicing which included producing false documentation and concealing the truth from his four associates, Beck regularly approved substantial GUA payments to the four companies. Beck then prepared fraudulent invoices from Creative Consultants and GA Christian Coalition for services that were never performed, and, at Beck's direction, his four associates paid the fraudulent invoices from the money they had been paid from GUA. Between February 2013 and August 2018, Beck stole more than $2,500,000 from GUA. (Source)

Former Executive Director Of Maryland Environmental Service Facing Charges For Fraudulently Obtaining $276,731+ From His Employer - October 5, 2021

MES, which was headquartered in Millersville, Maryland, generated its operating funds from fees charged to governmental and private clients for its services, as well as from federal grants and funding from federal agencies, including the Environmental Protection Agency, the U.S. Department of the Interior, and the U.S. Department of Transportation. MES functioned as an independent state corporation which did not pay its employees according to the state government pay scale, but did require its employees to comply with state travel regulations, annual leave policies, and policies regarding compensatory leave, and time and attendance reporting. McGrath resigned from MES as of May 31, 2020, to become the Governor's Chief of Staff effective as of June 1, 2020.

From March 2019 through December 2020, McGrath personally enriched himself by using his positions of trust as the Executive Director of MES and the Chief Of Staff for the Governor of Maryland to cause MES to make payments to McGrath, or on his behalf, to which he was not entitled.

McGrath caused MES funds to be paid to a museum where he was a member of the Board of Directors instead of using his personal funds to pay his pledge to the museum.

McGrath caused the MES Board of Directors to approve paying McGrath a $233,647.23 severance payment upon his departure from MES by falsely telling them that the Governor was aware of and approved the payment. McGrath caused MES to pay tuition benefits for McGrath after he left MES by personally approving reimbursements for payments. (Source)

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

Florida Nurse Pleads Guilty To Tampering With Intensive Care Unit Patient's Medication - October 28, 2021

On January 30, 2020, Jerome Clampitt, a registered nurse, was working a night shift in the intensive care unit of a hospital in Jacksonville. A patient under Clampitt's care was prescribed and receiving an intravenous dose of fentanyl, along with other medications for anesthesia. Two fellow employees saw Clampitt using a syringe to inject a substance into the device that dispensed fentanyl into the patient, when there was no medically valid reason for Clampitt to do so. Laboratory testing eventually determined that the patient's dose of fentanyl had been diluted with saline.

When interviewed by law enforcement officers, Clampitt eventually admitted that he had diverted drugs from patients at the hospital for personal use.

An audit of hospital records showed multiple discrepancies in Clampitt's handling of controlled substances during the time he worked for the hospital. Investigators later learned that in 2019, a separate hospital had employed Clampitt and discovered discrepancies in its records that suggested he might have been diverting drugs for his own use. That hospital fired Clampitt after he refused to submit to a drug test. (Source)

3 Former Medical Center Employees Stole Medical Records To Start New Clinic & Pharmacy - October 27, 2021

The University of Mississippi Medical Center (UMMC) hired Dr. Sullivan in 2014 to head its Hemophilia Treatment Center. Sullivan agreed to refrain from taking or using patient information for his own benefit, including soliciting patients for his own independent practice. However, in January 2016, Sullivan began arranging to start his own for-profit hemophilia clinic and pharmacy.

Over the course of the next few months, Sullivan coordinated with other UMMC staff (Co-Defendants Linnea McMillan, Kathryn Stevens) to prepare for the new clinic's opening. This included compiling UMMC patient records into a spreadsheet they called "the List." This spreadsheet included patients' birthdate, diagnosis, prescriptions, dose and frequency, insurance, pharmacy and home and mobile telephone numbers.

Sullivan resigned from his position at UMMC in June 2016, and then used the records stolen from UMMC to solicit these patents to continue their treatment at Sullivan's new clinic. Sullivan recruited at least 20 UMMC employees to work for him at his new clinic, and the majority of UMMC's hemophilia patients followed their physicians to his clinic. (Source)

Former Hospital Employee Used 700+ Patient Information For Personal Gain - October 22, 2021

On September 10, 2021, UNC Hospitals learned that one of its employees was using patient information for personal financial gain. The employee was responsible for handling payments from patients for services rendered by certain clinics of UNC Hospitals. The now former employee had access to patient demographic information including Social Security numbers, as well as copies of patient driver's licenses and insurance cards.

UNC Hospitals has confirmed that this former employee used some patients' demographic and financial information to fraudulently obtain goods or services. (Source)

Former Nurse Working For Senior Care Facilities Pleads Guilty To Stealing Drugs From Elderly Patients - October 15, 2021

Angele Mohler worked as a nurse for senior care and nursing facilities from 2018 to 2021. She used her position of trust to steal pain medications like oxycodone, hydrocodone, and morphine from vulnerable patients. After taking the drugs for her personal use, Mohler would often destroy or modify the patient's records to cover up the thefts. This meant the patient's records would show Mohler had given him or her pain medication, when in fact they had often suffered without it.

Mohler is one of several medical professionals recently charged with stealing medication from patients. (Source)

Former Medical Center Nurse Charged With Tampering With Hospitals' Fentanyl Supply - October 4, 2021

Between January 2020 and April 2020 Faith Naccarato, allegedly used her fingerprint to remove vials of fentanyl from an automated dispensing cabinet at Menorah Medical Center in Overland Park. She is accused of replacing the fentanyl with an alternant liquid substance before placing the vials back in the cabinet. (Source)

TRADE SECRET THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

ProofPoint (Insider Threat Monitoring Vendor) Employee Steals Confidential Sales Data To Give His New Employer A Competitive Edge - July 30, 2021

ProofPoint is an Insider Threat Monitoring / Data Loss Prevention Vendor.

Proofpoint has sued a former high-ranking channel executive to prevent him from working for rival Abnormal Security and misusing confidential information he allegedly took from Proofpoint.

Proofpoint claims ex-Director of National Partner Sales Samuel Boone shared with Abnormal's sales leaders and engineers a 'battlecard' that outlines Proofpoint's strategies for competing against Abnormal's sales tactics.

Before heading out the door, Boone pocketed a USB thumb drive to which he covertly misappropriated dozens of Proofpoint's most closely guarded proprietary documents,Proofpoint wrote in a filing with the U.S. District Court in Texas.

Abnormal Security wasn't named as a defendant in the court filings, though Proofpoint alleges that Abnormal tried to poach at least six Proofpoint employees – including account executives and a senior vice president – since October 2020 in violation of their post-employment confidentiality agreements. Abnormal can scan customers' delivered emails in programs like Office 365 for certain types of threats. (Source)

Former Employee Arrested For Stealing Personal Information Of 600,000+ From Company And Selling It Online To Pay For Gambling - October 8, 2021

The 27-year-old suspect was charged with accessing a computer system without authorization. The arrest was made a month-long investigation when the company was alerted to the sale of data claimed to have come from its database. Police working with the company's technicians identified the former employee as a suspect.

During his interrogation, the suspect admitted he had accessed the company's computer system and stolen data containing the personal information of the 600,000 people. He said he sold it for 300,000 baht in digital currency, and spent the money on online gambling. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Credit Union Operations And Marketing Director Charged With Embezzling $242,000 - October 28, 2021

Monica Jackson was the Operations and Marketing Director at Lifeway Credit Union in Nashville. In that role, she was part of the management team, and she oversaw the credit union's operating activities, including lending decisions and the decision to order cash. She also had access to Lifeway's cash vault.

Between October 2016 and February 2021, Jackson embezzled approximately $242,156 from the credit union using a variety of methods, including by stealing cash out of the vault. Jackson concealed these cash thefts from the vault, totaling more than $47,000, by placing small bills, such as one-dollar bills, in "bands" of larger bills, such as $20 or $50 bills, to make it appear as though each "band" of larger bills was full. Another method employed by Jackson was to open lines of credit in the names of family members and then transfer the funds to accounts she controlled. Jackson took approximately $167,312 by this method.

Jackson also made fraudulent transfers totaling $27,435 to herself from the account of a deceased credit union member. Jackson used her administrative authority to lock access to the accounts she was using to commit the fraud so that other bank employees could not see those accounts. (Source)

Former Bank Teller Sentenced To Prison For Role In $341,000+ Bank Fraud Conspiracy - October 22, 2021

Valnardia Novas was a bank teller at TD Bank and was paid to participate in this scheme. In September and October 2017, co-conspirators instructed Novas to fraudulently withdraw more than $300,000 in the form of bank checks and cash.

This case was the result of a larger investigation into multiple schemes to withdraw funds, in the form of checks and cash, from customer accounts at several financial institutions. The organizers of the scheme paid individuals to go into banks with falsified identification documents in the names of bank customers and request withdrawals from those customers' accounts. Bank tellers were also recruited to accept the falsified identification documents without scrutiny and facilitate the withdrawals. The fraudulently-obtained funds were then negotiated through accounts at other financial institutions that had been opened in the names of fictitious business entities. (Source)

Bank Tellers Involved In $357,000+ Bank Fraud Conspiracy - October 20, 2021

This case was the result of a larger investigation into multiple schemes to withdraw funds, in the form of checks and cash, from customer accounts at several financial institutions. The organizers of the scheme paid individuals to go into banks with falsified identification documents in the names of bank customers and request withdrawals from those customers' accounts.

Bank tellers were also recruited to accept the falsified identification documents without scrutiny and facilitate the withdrawals. The fraudulently-obtained funds were then negotiated through accounts at other financial institutions that had been opened in the names of fictitious business entities.

Lajerran Long was paid to recruit a teller at Santander Bank to participate in this scheme. In December 2017 and January 2018, co-conspirators utilized this bank teller to fraudulently withdraw more than $800,000. The majority of the fraudulently-obtained funds were subsequently recovered by the bank.

Long was also ordered to pay restitution of $357,333 and forfeiture of $5,000. (Source)

Former Bank Employee Pleads Guilty To Conspiracy To Commit $250,000+ Of Bank Fraud - October 19, 2021

Danielle Bartley, a former Capital One Bank employee from Silver Spring, Md., pleaded guilty to taking part in a conspiracy that compromised the account information of at least nine bank account holders and sought at least $253,000 in fraudulent withdrawals and transfers.

Bartley admitted in entering her guilty plea, at the time of the conspiracy in 2017, she was a branch associate in Washington, D.C. Between June and August 2017, Bartley and her co-conspirators, including Krishna Jannor-John Marsh, posed as nine different actual bank account holders and sought at least $253,000 in fraudulent withdrawals and transfers. They succeeded in obtaining one $50,000 wire transfer using personal identifiers of an account holder that Marsh purchased on the dark web. Other attempts were stopped, including one by an alert teller. (Source)

Former Bank Teller Pleads Guilty To Embezzling $63,000+ Of Customer Funds - October 13, 2021

Between December 3, 2018 and December 6, 2019, Demetria Silvio forged approximately 66 checks that were drawn on IberiaBank accounts belonging to five customers. Silvion deposited the fraudulent checks into her own bank accounts with Chase Bank and Capital One. Through this scheme, SILVIO embezzled approximately $63,059.82. (Source)

Former Bank Employee Pleads Guilty To Role In Two Fraud Schemes - October 7, 2021

Between approximately June 2014 and November 2018, Richard Harris engaged in two separate wire fraud conspiracies. In the first conspiracy, Harris exploited her position at Nantucket Bank by obtaining personally identifiable information of a customer and surreptitiously taking photographs of the victim's account information. Harris then shared that information with co-conspirators who attempted to transfer funds out of the customer's bank account without authorization.

In the second conspiracy, Harris helped perpetuate a fraudulent lottery scheme targeting at least 13 victims. According to the charging documents, victims were contacted by co-conspirators via phone and informed that they won large prizes, and that in order to receive the funds they needed to pre-pay taxes on their winnings. In reality, no such prizes existed. After victims made an initial payment, they were advised that additional advance payments were required for expenses such as insurance, transportation or other international customs' fees. Harris and her co-conspirators transferred proceeds of the scheme to associates in Jamaica and in the United States. (Source)

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

Former Employee Sentenced To Prison For Embezzling $1 Million+ For Personal Use (Bought BMW, Porsche, Etc.) - October 29, 2021

Justina Holland was employed at a local business where she had access to the bank and credit accounts of the business and its owner. From March 2015 through June 2018, Holland used her position to embezzle more than $1 million from her employer and the employer's owner. Holland's scheme consisted of three parts:

First, Holland embezzled more than $300,000 by taking funds from various company checking and IRA accounts and by manipulating the company payroll system to receive additional salary payments.

Second, Holland engaged in more than $700,000 of credit card fraud by making unauthorized purchases using the victim's credit cards, which she paid by making unauthorized transfers from her employer's various bank accounts. Holland also opened a credit card account in the victim's name by using his Social Security number and then used that card to make more than $196,000 in purchases for herself, including visits to a local theme park. Holland used her employer's bank accounts to pay the bills for that credit card.

Lastly, Holland used her minor son's Social Security number to obtain financing to purchase a BMW and a Porsche. Holland used funds from her employer to make some of the car payments for her vehicles.

Holland covered up her embezzlements by providing her employer with false spreadsheets that concealed her spending, among other things. (Source)

Former Staples Sales Manager Pleads Guilty To $81,000+ Visa Gift Card Fraud Conspiracy - October 26, 2021

Ricardo Voltaire was a sales manager at Staples locations in Dedham and Braintree in Boston. On at least 60 occasions, Voltaire processed fraudulent Staples' store credit account applications that were submitted by Wagner Sozi and his co-conspirator, each of which contained stolen personal identifying information of another individual. Voltaire knew that his co-conspirators were not in fact the individuals named on the applications and opened store credit accounts under the stolen identities, which were then used to purchase more than $81,000 in Visa gift cards. Voltaire accepted approximately $8,000 in kickbacks from Sozi and his co-conspirator. (Source)

Former General Manager For Real Estate Company Pleads Guilty To $23 Million Fraud Scheme To Live Luxury Lifestyle - October 26, 2021

From November 2015 to July 2018, Serena Shi was the general manager of Global House Buyer LLC (GHB), a China-based real estate company that had an office in Los Angeles. Shi identified approximately 47 acres of land in Coachella to build Hyde Resorts and Residences Coachella Valley.

Shi contacted representatives of Dakota Development, a real estate development subsidiary of the Los Angeles-based lifestyle hospitality company SBE Entertainment, about using SBE's "Hyde" brand, which was a luxury hotel and nightlife brand owned by SBE. Through these discussions, Shi reached an agreement with Dakota Development that the Hyde Development would be developed under SBE's brand name "Hyde."

Hyde Resorts was supposed to be a 207-unit luxury condominium and hotel complex with 95,000 square feet of conference facilities, a pool, spa, fitness center and other amenities.

Shi solicited investments in the Hyde complex from victims, the majority of whom were Chinese investors, by giving sales presentations at hotels and contacting victims over WeChat, a Chinese messaging, social media and mobile payment application.

To induce the victims to invest in the Hyde complex, Shi made false and fraudulent statements to them, including that their money only would be used to fund the Hyde development project, even though she intended to use victims' money for her own personal expenses.

After Shi received the victim funds, she spent nearly $300,000 in victim funds to purchase two luxury cars. She also spent approximately $2.2 million in victim funds at a company that provided luxury travel and concierge services. Shi also admitted spending almost $800,000 in victim funds at a full-service styling agency in Beverly Hills, as well as hundreds of thousands of dollars of victims' money on high-end clothing designers, restaurants and other stores. (Source)

Former Chief Financial Officer For Business Found Guilty Of $920,000 Employment Tax Fraud To Personal Use - October 25, 2021

Rochelle Anglin was the Controller and Chief Financial Officer for Atmospheric Technology Services Company (ATSC) located in Norman, Oklahoma. In that role, Anglin was responsible for withholding from employee wages and paying to the IRS payroll taxes, which included Social Security and Medicare taxes and federal income taxes.

From the first quarter through the third quarter of 2018, Anglin did not pay to the IRS nearly $920,000 in payroll taxes, which had been withheld from employees. At the same time these taxes were not paid, Anglin approved thousands of dollars of business expenditures, including salary and bonuses for herself and other executives. (Source)

Former IT Manager Arrested For Wire Fraud & Money Laundering After Embezzling $370,000 from Non-Profit Organization - October 22, 2021

Kyriakos Kapiris was arrested for allegedly embezzling approximately $370,000 from a non-profit organization.

From April 2015 to May 2020, Kapiris worked as the Information Technology (IT) manager at the non-profit organization. As part of his responsibilities, the organization provided Kapiris access to two company credit cards to purchase IT equipment and services as needed.

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

Kapiris linked the three vendor accounts to several of his own personal accounts at Bank of America into which he transferred the fraudulent proceeds. Kapiris then used the stolen funds for personal expenses including a $19,250 payment to a contractor that Kapiris hired to build a new residence in Northborough. (Source)

Former Payroll Administrator Sentenced To Prison For $1.6 Million+ Fraud Against Employer For Over 7 Years - October 22, 2021

According to the government's evidence, except for brief periods, Eleanor Milligan worked from 1998 to 2016 for a company based in Washington, D.C.

Beginning in at least or about August 2009, and continuing until in or about March 2016, Milligan used her fellow employees' names and personal identifying identification without authority to transmit false payment requests to herself through the employer's payroll processing system. In total, Milligan caused more than $1.5 million in fraudulently obtained payments to be direct-deposited into accounts under her control and otherwise paid for her benefit.

In total, Milligan stole money on more than 500 occasions, totaling $1,618,082. In addition, when she was nearly caught, Milligan created a fake email and mailing address in the name of another employee, whose identity she used to hide her scheme and that she was actually receiving the fraudulent payments herself. (Source)

National Labor Organization Employee Pleads Guilty To Embezzling $275,000+ From Union For Personal Expenses - October 20, 2021

From October 2014 through June 2018, Donnell Owens worked as a Secretary to the Director of Communications at the American Federation of Government Employees (AFGE), a labor organization headquartered in Washington, D.C. During this period, Owens embezzled approximately $275,524 in AFGE funds for his use and the use of others.

For example, Owens submitted false and fraudulent check requests for payments related to services, such as photography and videography, that were purportedly provided by alleged vendors. As a result of these submissions, AFGE funds were subsequently disbursed. These check requests listed fictitious dollar amounts for fake work assignments supposedly performed by vendors, who were not actually hired by AFGE. In fact, the purported vendors who allegedly performed the fake work assignments were really friends and associates of Owens, who he recruited as part of his illegal scheme.

Owens also had access to an Amazon account and a union credit card linked to it. During the scheme, Owens also used this account and linked credit card to embezzle items and make dozens of unauthorized personal purchases, including clothing, shoes, jewelry, and party supplies. Additionally, Owens used union credit cards to purchase items from other online retailers for personal use, including T-shirts for his online business, microphones, and flowers.

To avoid detection and cover up the fraud, Owens provided falsified signatures, fraudulent expense vouchers, and altered receipts for these items. However, the investigation revealed photos of Owens, his family members, and associates wearing the clothing purchased on Amazon with the union credit card on social media accounts belonging to the defendant. (Source)

Former Phone Company Employee Given Probation For Role In Cell Phone Sim Swap Scam Bribery Conspiracy - October 20, 2021

A SIM Swap scam is a cellular phone account takeover fraud that results in the routing of a victim's incoming calls and text messages to a different phone. Once a perpetrator is able to swap the SIM card, it is likely he is able to obtain access to a victim's various personal accounts, including email accounts, bank accounts, and cryptocurrency accounts, as well as any other accounts that use two-factor authentication.

From August 2017 until November 2018, Stephen Defiore worked as a sales representative for Phone Company A. In that capacity, Defiore had access to the accounts of Phone Company A's customers, including the ability to switch the subscriber identification module (SIM) card linked to a customer's phone number to a different phone number.

Between October 20, 2018, and November 9, 2018, Defiore accepted multiple bribes, typically in the amount of approximately $500 per day, to perform SIM swaps of Phone Company A customers identified by a co-conspirator. For each SIM swap, a co-conspirator sent Defiore a customer's phone number, a four-digit PIN, and a SIM card number to which the phone number was to be swapped. In total, Defiore received approximately $2,325 in a series of twelve payments. (Source)

Former Casino Employee Sentenced To Prison For Embezzling $315,000+ - October 18, 2021

In 2008, Jennifer Lynn Boutto, 33, began working as a reservationist at the Fortune Bay Resort Casino, which is owned and operated by the Bois Forte Band of Chippewa. Boutto later received a promotion to Front Desk Supervisor, a position that allowed her to issue cash refunds without direct supervision. Between January 2013 and October 2019, Boutto used her position at Fortune Bay to steal money by issuing false cash refunds against the invoices of previous Fortune Bay customers. Boutto would then access the Fortune Bay vault and retrieve the falsely refunded amount. In total, Boutto executed the scheme 2,994 times and stole $315,739.87. (Source)

Former Executive For Publication Company Sentenced To Prison For Embezzling $48 Million+ For Personal Expenses - October 18,2021

Nestor Charriez was a longtime senior employee of Victim-Company 1, a publication company based in New Jersey. Charriez's financial responsibilities at Victim-Company 1 included overseeing and managing employee payroll. Charriez would submit Victim-Company 1's payroll information to an outside payroll company, which would process Victim-Company 1's payroll requests.

Beginning as early as 2002 through June 2019, Charriez defrauded Victim-Company 1 by embezzling millions of dollars through unauthorized "bonus" payments to himself. He submitted false payroll instructions to Victim-Company 1's outside payroll provider, indicating that Charriez was entitled to massive bonuses – hundreds of thousands of dollars at a time – which Victim-Company-1 had not approved.

Charriez carried out this scheme on numerous occasions over nearly two decades. In total, Charriez stole more than $48 million from Victim-Company 1. Charriez spent the money he stole on personal expenses. (Source)

Former Executive Director For Non-Profit Organization Sentenced To Prison For Misappropriation Of $500,000+ For Personal Use - October 15, 2021

From 2011 to 2016, Stuart Nitzkin worked as Executive Director of an Illinois-based non-profit organization whose mission was the rehabilitation of physically and psychologically challenged children. Nitzkin knowingly submitted to the organization invoices and receipts for payment and reimbursement of expenses that Nitzkin claimed were incurred on behalf of the organization. In reality, Nitzkin knew the expenses were actually incurred by Nitzkin for his and others' personal benefit.

The expenses included luxury vacations for Nitzkin and his family to Nevada, Florida, Ireland, and Puerto Rico, personal golfing expenses, tickets to professional sporting events, personal medical expenses, real estate taxes for his family residence, health club dues, and household goods. Nitzkin also pocketed cash from the organization's fundraising events and took money from the charity's bank accounts through ATM and other withdrawals, all for his personal benefit. (Source)

Former Financial Controller For Dining Club Sentenced To Prison For Embezzled $300,000+ For Personal Use - October 15, 2021

Isabelle Garcia began work in 2006 as the financial controller for the George Town Club, a private dining club located in the District of Columbia. She was responsible for maintaining the club's financial affairs and had a great deal of discretion. From December 2006 to September 2013, Garcia used her control over financial accounts to make payments to herself and to third parties for her personal benefit. Through her scheme, Garcia wrongfully obtained $300,442. (Source)

Former Finance Manager For Construction Company Embezzles $500,000+ - October 15, 2021

William Tempel Construction entered into a contract to build a residence for a client. Beginning in May 2013, subcontractors submitted invoices directly to William Tempel Construction. Lynn Tempel provided the client invoices in which she had fraudulently inflated the amount of payment required. William Tempel Construction received approximately $4.41 million from the client for the construction of the residence. The investigation determined that LunnTempel falsified, altered and inflated about 153 subcontractor invoices, and stole than $500,000. (Source)

Former Bookkeeper Sentenced To Prison For $1.5 Million+ Fraud For 10 Years To Pay Credit Card Bill - October 12, 2021

Between 2007 and 2017, Paula Hise used her trusted position as a bookkeeper for her employer to steal funds from her employer by obtaining an unauthorized credit card, using that credit card for personal purchases, and then paying the balance of the credit card using her employer's business checking account. Hise concealed her crime by creating false entries in the business' account ledgers, creating false accounting reports, and providing false information to her employer. (Source)

Former Office Manager Sentenced To Prison For Embezzling $1 Million+ From Employer To Make Mortgage & Truck Payments, Traveling - October 7, 2021

From 2013 to 2019, Richard Clark was employed as an office manager for two family-owned businesses in Lenoir, and was responsible for handling the companies' bookkeeping and financial records, making payments to vendors and the IRS, and reconciling the companies' bank accounts. Clark used his position and his access to the companies' financial records and bank accounts to embezzle more than $1 million from his employers. Court records show that Clark stole money from a company bank account the owner had directed Clark to close. Instead of closing the account, Clark used it to steal from his employer, by instructing customers to make payments to that account.

Clark also admitted that he laundered the funds he embezzled from his employer by withdrawing customer funds from the company's bank account through multiple fraudulent checks payable to himself, which he deposited into personal bank accounts. Clark then used the stolen funds to pay for his personal lifestyle, including to make payments for his home mortgage, to make auto loan payments for an F-150 truck and other vehicles, to install a home theater system, and to pay for travelling and shopping expenses, among other things. (Source)

4 Former Utility Company Employees Plead Guilty In $300,000 Bribery And Kickback Scheme - October 4, 2021

4 company managers employed in the facilities department of the utility company, steered contracts to certain Long Island-based contractors, in exchange for hundreds of thousands of dollars in bribes and kickbacks. The utility contractor secured more than $50 million in facility maintenance contracts from the contractor that was paying bribes to the 4 company managers.

The bribe payments to the defendants included cash, the purchase of a recreational vehicle, home improvements, landscaping and an overseas vacation. As part of the investigation, agents recovered approximately $300,000 in cash from a safe deposit box held by one of the managers. (Source)

Former Dental Practice Office Manager Sentenced To Prison For Defrauding Medicaid Of $813,00+ Through False Billing Scheme - October 1, 2021

Mahsa Azimirad was the marketing and operations manager for Universal Smiles, a dental practice in Northwest Washington. Through Universal Smiles, she and Bilal Ahmed (Ran Dental Practice) engaged in a scheme to enrich themselves by defrauding D.C. Medicaid, a health care benefits program jointly funded by the federal government and the District of Columbia to provide health care services to residents who meet the income qualifying requirements. As part of the scheme, Ahmed applied to be a Medicaid provider. Once approved to bill Medicaid, Azimirad and Ahmed then billed D.C. Medicaid for thousands of provisional crowns, a significant number of which were not provided to the Medicaid patients. From Aug. 9, 2012, through Feb. 26, 2014, D.C. Medicaid paid Universal Smiles approximately $5.4 million for provisional crowns. Of the $5.4 million that D.C. Medicaid paid for provisional crowns, Azimirad received approximately $813,184. (Source)

UNIVERSITIES / EDUCATION / SCHOOLS

Former University IT Department Employee Charged With Hacking & Leaking COVID Vaccine Exemption Requests - October 21, 2021

Alejandro Benitez is accused of publishing a list of Chico State students who applied for a religious exemption from the university's COVID-19 vaccine requirement. The spreadsheet posted online included requests from 130 students. Student names and other personal information were listed in 18 of the entries.

Benitez worked for Chico State's IT department and hacked into multiple computers to access the information. The leaked data first came to light when a Sacramento newspaper wrote an article about the spreadsheet which had been posted to several online forums. A Chico State professor had alerted the paper in the hopes of protecting affected students from civil rights and privacy violations. (Source)

DATA / COMPUTER / NETWORK MISUSE & SABOTAGE

Fired IT Administrator Sabotages 2 Employers Computer Systems After Being Fired (Wiping Data, Changing Passwords) - October 6, 2021

At the beginning of the year on January 16, Adam Georgeson downloaded and deleted data from computers belonging to Welland Park Academy in Market Harborough, Leicestershire, and changed passwords of staff members. As a result of his actions, the school's computer systems could no longer be accessed and remote learning was impacted at a time when pupils were at home due to the Covid-19 pandemic. Georgeson had been working as an IT technician at the school but had been fired at the time of the attack.

On January 21, while employed at an IT company in Rutland, Georgeson was arrested for his actions on the school's network and was fired in February.

On March 9, the IT company reported unauthorized activity on its network. Apart from changing passwords that locked users out, Georgeson also modified the phone system used to contact customers. (Source)

Former Employee Hacked Flight School Computer System And Cleared Planes With Maintenance Issues To Fly - October 12, 2021

Lauren Lide who used to work for the Melbourne Flight Training school, resigned from her position of Flight Operations Manager at the end of November of 2019, after the company fired her father. Months later, she allegedly hacked into the systems of her former company, deleting and changing records, in an apparent attempt to get back at her former employer. According to the school's CEO, this could have put pilots in danger.

Derek Fallon, the CEO of Melbourne Flight Training called the police on January 17, 2020, and reported that five days before, he logged onto his account for Flight Circle, an app his company uses to manage and keep track of its airplanes, and found that there was missing information. Fallon found that someone had removed records related to planes with maintenance issues and reminders of inspections had all been deleted, "meaning aircraft which may have been unsafe to fly were purposely made 'airworthy,'" according to a document written by a Melbourne Airport Police officer.

The owner of Flight Circle found that the records had been tampered with by someone who logged in with the credentials of Melbourne Flight Training's current Flight Operations Manager.

Police investigators then obtained information related to the IP address used to access that account, and found that it belonged to Hampton Lide, the father. The investigators also subpoenaed Google for information about a Gmail account used to log into the Flight Circle app, and found that the email address belonged to a user with the name "The Lides." Hampton Lide would later tell investigators that this was the family's email address. (Source)

WORKPLACE VIOLENCE

Philadelphia Hospital Employee Shoots Co-Worker - October 6, 2021

The gunman who fatally shot his co-worker at a Philadelphia hospital early Monday fled the scene in a U-Haul truck before firing 76 rounds at police officers during a gunfight, according to a report.

The suspect, Stacey Hayes shot his co-worker six times on the ninth floor of Thomas Jefferson University Hospital just after midnight.

Hayes and the victim knew each other, though police have yet to formally reveal a motive. (Source)

2 U.S Postal Service Employees Killed By Another Employee - October 12, 2021

2 U.S Postal Service employees were killed at a Memphis, Tenn., post office and the suspected shooter, also an employee, died from a self-infliced gunshot, authorities said. Authorities have not yet provided a motive for the shooting. (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 (**3,00+ 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 **640+** 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