<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>Message from the Chief</td>
</tr>
<tr>
<td>03</td>
<td>Organization Chart of CI</td>
</tr>
<tr>
<td>04</td>
<td>2023 Snapshot</td>
</tr>
<tr>
<td>05</td>
<td>Closing the Tax Gap</td>
</tr>
<tr>
<td>06</td>
<td>Combatting Fraud &amp; Money Laundering</td>
</tr>
<tr>
<td>07</td>
<td>Assisting in the Fight</td>
</tr>
<tr>
<td>08</td>
<td>Catching Criminals Utilizing False Claims &amp; Credits Detecting Fraudulent Tax Refunds</td>
</tr>
<tr>
<td>09</td>
<td>Cybercrimes &amp; Tracking Funds Through Cryptocurrencies Fighting Fentanyl &amp; Exploitation on the Dark Web Marketplace</td>
</tr>
<tr>
<td>10</td>
<td>Intercepting Threats to Our National Security Disrupting &amp; Dismantling Transnational Criminal Organizations</td>
</tr>
<tr>
<td>11</td>
<td>Global Collaboration &amp; Enforcement Contributing to the Community</td>
</tr>
<tr>
<td>12</td>
<td>Protecting Our Seniors from Scams Safeguarding Covid Relief Funds</td>
</tr>
<tr>
<td>13</td>
<td>Rooting Out Corruption Recovering Losses for Victims</td>
</tr>
<tr>
<td>14</td>
<td>Securing the Integrity of the Financial System</td>
</tr>
<tr>
<td>15</td>
<td>Field Office Map</td>
</tr>
</tbody>
</table>
I am so proud of the tremendous work done by the men and women of IRS Criminal Investigation (CI). Financial crime continues to evolve at a rate that challenges law enforcement daily. We will never investigate our way out of any one particular type of crime, so where we spend our time and resources must be methodical in an effort to protect the integrity of the financial system. Our relevance within the enterprise is significant, and the deterrent effect provided by showing the consequences for being willfully noncompliant is real and impactful. This year, we focused on quality and impact in our case selection, and I could not be prouder of the investigations our agency brought to bear.

Tax and tax-related crimes continue to dominate the division’s investigative inventory. Our priority must continue to be tax, as we are the only agency that can investigate and recommend violations involving federal income tax crimes. These investigations create deterrence, which is critical to encouraging tax compliance. The revenue collected by the IRS each year funds nearly 96% of our government. Our investigative mission is important, and there is no better investment in government than investing in CI!

We continue to lead the way in our investigative efforts involving digital assets, and we are reaping the benefits of early investment in our cyber capabilities and training. Our partnerships with the private sector created opportunities for us to solve the most complex crypto-related crimes in the world. We remain focused on stopping those who attempt to exploit new technology for nefarious purposes, mitigating illicit finance, and identifying national security risks. We know that digital assets provide opportunities for responsible financial innovation, and most people using cryptocurrency do so for legitimate purposes. But, we also know that digital assets pose a risk of facilitating money laundering, cybercrime and ransomware, narcotics, human trafficking, terrorism, proliferation financing, and tax crimes. Chain-hopping and token swapping have become common digital assets techniques used to make following the digital money trail more difficult, but not impossible.

Our responsibility to be a meaningful player in the international tax and law enforcement community remains high. We are proud members of the Joint Chiefs of Global Tax Enforcement (J5), which just celebrated five years together. We deliver trainings to representatives from multiple countries across the globe. In May 2023, CI delivered blockchain analysis tools and cyber training to Ukrainian law enforcement agencies. A couple of months later, we partnered with the UK and The Netherlands to provide a second round of training to Ukrainian law enforcement officers. The training focused on cryptocurrency and blockchain tracing.

I’m proud to say that our role in national security continues to be a priority for CI as well. In collaboration with agency partners, we leverage our unique investigative authorities to identify, disrupt, and defeat those who engage in activities that degrade our financial integrity, distort markets, and victimize our citizens. We continue to be a key player in sanctions-related enforcement efforts through Task Force Kleptocapture, which targets Russian oligarchs and other would-be sanctions evaders. Building on past disruptions of terrorist organizations like Hamas using cryptocurrency to fundraise, CI continues to prioritize cases that have significant impacts on preventing terrorist organizations from being able to fund their activities.

While I look back on a year like 2023 full of our many organizational successes, I also could not be more excited with the work we have already begun doing in 2024. I could not be prouder of the men and women in IRS Criminal Investigation.

Jim Lee – Chief
2023 SNAPSHOT

DIRECT INVESTIGATIVE TIME SPENT

INVESTIGATION SOURCES

STAFFING*

CI's staffing levels are by fiscal year and reflect an actual count of employees based on the Employee Master Database as of FY19.

Tax Fraud Identified
$5.5B

Other Identified Financial Crimes
$31.6B

Warrants Executed
1334

Referred For Prosecution
1838

Conviction Rate
88.4%

Convictions
1508

Petabytes Of Digital Data
1.71
Voluntary compliance is the backbone of the U.S. tax system. The IRS relies largely on taxpayers to report their income, calculate the amount of tax they owe, and remit that amount to the IRS through withholding or other payments. The gross tax gap is the difference between the amount of tax owed by taxpayers for a given year and the amount of taxes paid on time for that same year. IRS projected the gross tax gap at $688 billion for tax year 2021 alone, which could result in approximately $7 trillion in lost tax revenue over the next decade. As one of the oldest federal law enforcement agencies, CI is the only federal law enforcement agency with jurisdiction to investigate federal tax crimes. CI is committed to reducing the tax gap by dedicating 70% of direct investigative time to tax investigations.

Targets of tax fraud investigations include individuals who deliberately underreport or omit income from their tax returns, such as high-income individuals who have a filing requirement but deliberately choose not to file returns and pay taxes owed. CI holds these tax evaders accountable, whether they are a TV personality who evades paying their tax obligations, or a taxpayer who embezles funds or fails to report millions earned in illegal Dark Web transactions.

With the increased use of digital assets in the mainstream economy, there has been a rise in digital asset tax investigations. These investigations consist of unreported income resulting from failure to report capital gains from the sale of cryptocurrency, income earned from mining cryptocurrency, or income received in the form of cryptocurrency, such as wages, rental income, and gambling winnings. CI is also seeing evasion of payment violations, where the taxpayer fails to disclose ownership of cryptocurrency in an attempt to shield holdings.

Promoters of overseas tax shelters or schemes develop sophisticated offshore structures, trusts, and bank accounts to unlawfully conceal millions of dollars of income from the U.S. Government. CI not only seeks to hold U.S. taxpayers taking part in these schemes responsible, but to pursue the promoters of the scheme, even if the promoter is an international tax advisor operating outside of the US border.

Businesses also contribute to the tax gap by concealing profits from the IRS in an attempt to evade taxes owed. In January 2023, William Chen, a New England restaurant owner, was sentenced to prison for utilizing “zapper” software to deliberately delete transactions from his business’ point of sales system and underreporting millions in gross receipts on his taxes. Even individuals who win big in the lottery, try to wiggle out of paying their fair share. In May 2023, Ali and Yousef Jaafara, father and son, were sentenced in a “ten-percenter” scheme, where they unlawfully claimed more than 14,000 winning lottery tickets for others and laundered over $20 million in proceeds, resulting in a federal tax loss of more than $6 million.

Some tax schemes have victims beyond the IRS. Employment tax fraud significantly contributes to the tax gap due to underreporting and underpayments. Employment tax fraud not only steals money from government coffers but also from hardworking employees. Employment tax fraud investigations include paying employees in cash under the table, filing false payroll tax returns, and failing to collect payroll tax from the employees. CI also investigates employers who withhold taxes from their employees’ paychecks but then use the funds for personal expenses or to enrich themselves. CI also seeks employers who withhold taxes from their employees’ paychecks but then use the funds for personal expenses or to enrich themselves. During the February 2023 sentencing of Kevin Shibliski, the judge stated imprisonment was necessary to send a deterrence message to two groups—business owners who willfully fail to pay their employment taxes and people who willfully fail to pay the IRS and use the tax funds for other purposes. Their actions have consequences, and they will go to federal prison.

Investigations that close the tax gap foster confidence in the tax system and compliance with the U.S. tax laws.
Money laundering occurs when criminals attempt to disguise the illicit nature of their funds by introducing it into the stream of legitimate commerce and finance.

In September 2023, Karl Greenwood, co-founder of OneCoin, was sentenced to 20 years in federal prison for marketing and selling fake cryptocurrency to millions of victims who invested over $4 billion worldwide. In that same month, four men in Arkansas were convicted of cheating victims out of more than $18 million that they laundered through a web of international bank accounts.

In June 2023, Rachael Winslow was sentenced to over 11 years in prison for her role in an international conspiracy to launder funds generated via boiler room fraud. Boiler room victims were led to believe there was legitimate investments in reputable companies, such as Facebook, Chesapeake Energy, or Toys R Us. In fact, the investments were worthless, and the boiler rooms defrauded the victims of more than $14 million.

The use of professional money laundering or third-party money launderers has expanded with technology. Third-party facilitators place illicit proceeds into businesses, financial institutions, brokerage firms, and physical assets to conceal the nature of the illicit profits. In December, Ian Freeman was convicted of a bitcoin money laundering scheme. Freeman laundered over $10 million in proceeds from romance scams and other internet fraud by exchanging U.S. dollars for bitcoin. To facilitate the money laundering, Freeman and his co-conspirators opened and operated accounts at financial institutions in the names of various churches and described the deposits as donations to try to conceal the true source of the funds.

In today’s technologically advanced world, criminal activity often crosses borders and can involve global financial crime. The crimes involve complex webs of offshore holdings and anonymous transactions, but CI traces the money each step of the way.

There are many faces to fraud, including tax, investment, healthcare, securities, and corporate fraud. However, the motive is always the same – money. CI’s premier financial investigators investigate fraud and the resulting money laundering that ensues.

Corporate fraud involves criminal violations committed by publicly traded or private corporations and their senior executives. Some specific criminal acts involving corporate fraud include falsifying, fabricating, or destroying company records. Fraudsters often use false information to complete tax returns, financial statements, and reports for regulatory agencies or investors. In June 2023, James Abrams, CEO of EthosGen LLC was convicted of 48 counts after a jury trial. Abrams provided forged documents and false information to induce several investors to invest in his company. The false documentation included forged teaming agreements, intellectual property licenses, tax returns, and financial statements that fabricated an existing customer base and inflated EthosGen LLC’s historical revenues, business activity, and profitability.

Fraudsters will look for opportunities to perpetrate a scheme in all industries. In April 2023, Julian Omidi was sentenced to seven years for defrauding Tricare and private insurance companies by fraudulently submitting nearly $120 million in claims under his 1-800-GET-THIN business. Over the summer, Jose “Chanel” Teran and Webster “Yenddi” Batista were sentenced to 10 years collectively for running one of the largest music royalty fraud schemes in history. Teran and Batista stole $23 million from YouTube for song royalties that belonged to Latin artists in numerous countries.

Money laundering occurs when criminals attempt to disguise the illicit nature of their funds by introducing it into the stream of legitimate commerce and finance. Criminals launder money through a wide variety of enterprises like banks, money transmitters, stock brokerage houses, casinos, and virtual currency exchanges. The flow of illegal funds around the world is estimated to be in the hundreds of billions of dollars. CI special agents are experts at uncovering money trails through traditional and virtual financial banking systems.

CI special agents are experts at uncovering money trails through traditional and virtual financial banking systems.
Today’s sophisticated schemes demand a highly skilled team made up of instructors, analysts, scientists, data experts, and professional staff to decipher complex financial crimes and support and train special agents for the fight.

CI special agents are sworn federal law enforcement officers who begin their training at the National Criminal Investigation Training Academy (NCITA), located at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia. After passing rigorous practical exercises and academic standards, special agents graduate from the nine-week FLETC Criminal Investigation Training Program (CITP) and continue onto CI’s specialized 16-week Special Agent Basic Training (SABT). NCITA instructors train special agents to investigate cases and complete investigative steps, such as interviewing, gathering evidence, applying methods of proof, and making recommendations for prosecutions. NCITA provides special agents the knowledge and skills needed as criminal investigators. NCITA also plays a vital role in advanced training and comprehensive continuing professional education courses to special agents and professional staff, which focus on emerging trends and issues within the law enforcement environment.

Nearly one-third of CI’s staff consist of professionals who work alongside special agents and provide support, guidance, and aid in accomplishing CI’s mission. Professional staff are on the front lines of case work and behind the scenes of every CI activity, whether it is an investigative analyst ensuring intelligence is accurate, administrative staff keeping the trains moving, computer specialists making sure CI has the necessary equipment, or our scientist and digital forensic team certifying evidence and linking that evidence to the criminals.

Digital Forensics supports special agents in the collection and analysis of digital evidence. During the last year, CI’s team seized over 1.7 petabytes of digital data from over 3,300 computer devices in support of investigations. Digital Forensics possesses the expertise to recover relevant evidence, including data that may have been encrypted, password protected, or hidden by other electronic means.

Since 1972, CI’s Center for Science and Design (CSD) has aided investigations through forensic testing and technical services. CSD’s scientific services include the ability to forensically process and analyze a wide variety of evidence, such as latent prints (finger and palm print development and comparison), questioned documents, ink chemistry, and DNA. In addition, CSD provides electronic enhancements, polygraph examination, and facial recognition. CSD’s design team simplifies the presentation of complex evidence for juries through compelling illustrations.

Workforce Development provides continuing education and career path opportunities to assist employees in meeting their career goals and finding career satisfaction. This section provides easy access to resources to help all employees stay balanced and engaged in their work and home life.

Equity, Diversity, and Inclusion Office (EDI) ensures that CI’s processes and programs are impartial and fair and that they provide equal possible outcomes for every individual. EDI creates and sustains a diverse, equitable, and inclusive environment that respects and accommodates every employee’s background, including race/ethnicity, sexual orientation, gender identity, and other protected statuses that make us all unique.

CI is honored to have a highly talented and diverse workforce that is dedicated to bringing criminals to justice. CI continually strives to maintain its status as a top-notch employer by supporting all its employees, providing developmental opportunities, generating paths to career advancement, and investing in each individual’s success.

"CI is honored to have a highly talented and diverse workforce that is dedicated to bringing criminals to justice."

"CI special agents are sworn federal law enforcement officers who begin their training at the National Criminal Investigation Training Academy."
Tax cheats pull out all the stops to compromise the integrity of the U.S. tax system. Whether it is someone who claims false tax credits or a team of individuals promoting and facilitating abusive tax schemes, it is CI’s job to catch the criminals who try to steer clear of paying their fair share. CI investigates promoters and the clients who willfully violate tax laws by participating in abusive tax schemes.

Tax credits that sound too good to be true are usually tax schemes pushed by promoters using improper methods to avoid paying taxes. Promoters peddle large tax deductions by abusing legitimate credits, such as fuel tax credits. Fuel tax credits (FTCs) are meant for off-highway business and farming use and are not available to most taxpayers. The FTC has been around for over 50 years, yet unscrupulous tax return preparers continue to abuse the credit. Individual tax returns requesting FTCs have significantly increased this filing season. In fiscal year 2023, CI initiated investigations involving more than $164 million of potentially fraudulent FTCs and seized funds totaling $1.49 million from these schemes.

In April 2023, five individuals were sentenced from six to 40 years in prison for their roles in a $1 billion biofuel tax fraud. The individuals conspired to appear as though they were producing and selling biodiesel to fraudulently claim more than $1 billion in refundable renewable fuel tax credits. As a result of the scheme, IRS paid out more than $511 million in credits to Washakie Renewable Energy, a Utah biodiesel company owned by Jacob and Isaiah Kingston.

Similarly, promoters tout abusive tax schemes under syndicated conservation easements. In September 2023, Jack Fisher and James Sinnott were found guilty of a fraudulent tax shelter scheme involving syndicated conservation easements, where they and others received more than $41 million in payments. Fisher and Sinnott designed, marketed, and sold over $1.3 billion in abusive syndicated conservation easement tax shelters. They grossly inflated the value of the easements so their high-income clients could claim fraudulently inflated tax deductions.

Other fraudsters make false claims on government grant programs. In December 2022, Christopher Condron was sentenced to seven years in prison for defrauding the U.S. Treasury of more than $50 million in tax-free energy grants as part of the American Recovery and Reinvestment Act of 2009. For nearly four years, Condron and his co-conspirators submitted fraudulent grant applications, falsely claiming entities had acquired, put into service, or started construction of energy property and sought reimbursement under the Act for costs they never actually incurred.

In April 2023, five individuals were sentenced from six to 40 years in prison for their roles in a $1 billion biodiesel fraud scheme. The individuals conspired to appear as though they were producing and selling biodiesel to fraudulently claim more than $1 billion in refundable renewable fuel tax credits. As a result of the scheme, IRS paid out more than $511 million in credits to Washakie Renewable Energy, a Utah biodiesel company owned by Jacob and Isaiah Kingston.

Similarly, promoters tout abusive tax schemes under syndicated conservation easements. In September 2023, Jack Fisher and James Sinnott were found guilty of a fraudulent tax shelter scheme involving syndicated conservation easements, where they and others received more than $41 million in payments. Fisher and Sinnott designed, marketed, and sold over $1.3 billion in abusive syndicated conservation easement tax shelters. They grossly inflated the value of the easements so their high-income clients could claim fraudulently inflated tax deductions.

Other fraudsters make false claims on government grant programs. In December 2022, Christopher Condron was sentenced to seven years in prison for defrauding the U.S. Treasury of more than $50 million in tax-free energy grants as part of the American Recovery and Reinvestment Act of 2009. For nearly four years, Condron and his co-conspirators submitted fraudulent grant applications, falsely claiming entities had acquired, put into service, or started construction of energy property and sought reimbursement under the Act for costs they never actually incurred.

Tax-related crimes make up the lion’s share of CI special agents’ investigations. Few crimes impact all American taxpayers like tax crimes, because tax revenue is the lifeblood of the government. It is estimated that fraudulent tax refunds cost Americans tens of millions of dollars each year.

By investigating bad actors who submit questionable refunds, file returns using stolen identities, use dishonest tax preparers, or claim false tax losses or dependent information, CI helps ensure the integrity of the tax system. CI special agents use their financial investigative expertise to uncover and quantify the seriousness of these schemes.

Questionable refund schemes often involve individuals who file numerous fraudulent tax returns for others, but sometimes they are based solely on false information submitted by a single taxpayer. CI special agents uncovered a years-long scam by Francis Burns, who filed false tax returns asking for refunds totaling more than $80 million. He claimed to be filing returns on behalf of an estate or a trust that did not exist. The returns contained fake Forms 1099s that falsely claimed significant sums of income were withheld for federal taxes by third parties, such as banks. In reality, Burns was unemployed, and there was no estate, no trust, and no income. While he did not receive the entire attempted refund amount, he spent the refunds he did receive on expenses including a lavish luxury home and a vehicle. He was sentenced to five years in federal prison and ordered to pay restitution. CI seized and forfeited a significant percentage of the assets Burns purchased with the fraudulent refunds.

Stolen identity refund fraud occurs when an identity thief uses a legitimate taxpayer’s identity to file a fraudulent tax return and to claim a refund. Generally, the identity thief will attempt to get a refund early in the filing season before the legitimate taxpayer files their tax return. CI aggressively investigates these cases and brings perpetrators to justice. In September 2023, Ariel Jimenez was sentenced to 12 years in prison for leading a tax fraud and identity theft conspiracy, where he obtained stolen identities of hundreds of minors and sold those identities to his tax clients so they could fraudulently claim them as dependents on their tax returns.

Return preparer investigations involve corrupt return preparers, who orchestrate the preparation and filing of false income tax returns for others. These preparers often claim inflated personal or business expenses, false deductions, excessive exemptions, and unallowable tax credits. The preparers’ clients may or may not know their tax returns were falsified. In North Carolina, two return preparers filed 1,000 false tax returns with the IRS that claimed approximately $5 million in fraudulent refunds. Both women behind this scheme were subsequently sentenced to federal prison and ordered to pay $5.2 million in restitution to the IRS. CI special agents investigate hundreds of these cases each year, helping ensure fairness in the tax system.
CI remains focused on stopping those who use digital assets to exploit technology for nefarious purposes, mitigate illicit finance and identify national security risks.

While digital assets provide opportunities for responsible financial innovation, safe and affordable financial services, they also pose risk of facilitating money laundering, cybercrime and ransomware, narcotics and human trafficking, terrorism, and proliferation financing.

Cryptocurrency continues to fuel cybercrime. CI Cybercrime Units have some of the top financial investigators in tracing cryptocurrency. Cybercriminals continue to create more sophisticated hacks and schemes in an attempt to outsmart the law to steal and launder massive amounts of cryptocurrency. CI has demonstrated its ability to pursue these criminals, no matter how complex the schemes, as shown in the Mt. Gox hack and the takedown of the illicit cryptocurrency exchange BTC-e. CI investigation of BTC-e exchange revealed illicit proceeds brought justice for more than 900 American victims and highlighted the importance of following the money trail no matter where it leads. The sentencing of Ionut-Razvan Sandu, a Romanian national, for laundering more than $3.5 million in fraudulent online auction proceeds brought justice for more than 900 American victims and highlighted the importance of working alongside law enforcement partners to pursue cybercriminals and bring them to justice.

CI special agents work tirelessly to combat money laundering, drug trafficking, and exploration on darknet marketplaces. CI’s Cyber and Forensic Services and Narcotics and National Security Section collaborated to initiate a Cyber-Organized Crime Drug Enforcement Task Forces (OCDETF) program to directly target criminals using the internet, darknet, and virtual currencies to conduct and profit from the sale of illicit narcotics. Our special agents are experienced in solving sophisticated cyber-related schemes and are up to the challenge of locating and apprehending criminals hiding in the digital world.

Under the Joint Criminal Opioid and Darknet Enforcement (JCODE) task force, CI and other law enforcement agencies around the world have joined forces to identify and take down criminals who use the darknet to buy and sell narcotics. CI plays an integral role in these investigations by following the money trail, whether it is in fiat currency or digital assets on the blockchain.

In May 2023, CI and JCODE partners announced the results of Operation SpecTor. The operation resulted in 288 arrests and the seizure of 117 firearms, 850 kilograms of drugs that included 64 kilograms of fentanyl or fentanyl-laced narcotics, and $53.4 million in cash and virtual currencies. Defendants in more than 100 cases were prosecuted for selling tens-of-thousands of counterfeited oxycodone pills containing fentanyl, in exchange for cryptocurrency via darknet marketplaces. Sadly, it is not only narcotics being trafficked on the darknet. Darknet sites also profit from human trafficking and the sexual exploitation of children. In July 2023, Vincent Galarza was sentenced to over 17 years in prison related to the Welcome to Video investigation. Galarza was one of 337 individuals arrested around the world. As a result of the investigation, law enforcement rescued 23 minor victims who were abused by users of the site.

CI continues to dedicate investigative time and expertise to tackle darknet and cryptocurrency crimes. In June 2023, CI also joined forces with other federal agencies to create the Darknet Marketplace and Digital Currency Crimes Task Force.
Criminals, corrupt entities, and foreign adversaries constitute significant financial threats to U.S. National Security. CI leverages our unique investigative authorities, in collaboration with agency partners, to identify, disrupt, and defeat those who engage in activities which degrade our financial integrity, distort markets, and victimize our citizens. CI participates in investigations involving terrorism, espionage, and other significant criminal activities undertaken on behalf of our nation's adversaries or international criminal organizations. Illicit actors engage in a wide variety of financial crimes and utilize their ill-gotten gains to cyber attacks, direct kinetic, and intelligence against Americans and our interests, both at home and abroad. In June 2023, three Russian nationals were charged with deploying LockBit ransomware and other cyberattacks against victim computer systems in the United States, Asia, Europe, and Africa. LockBit actors allegedly executed over 4,400 attacks against victims around the world, issuing over $100 million in ransom demands and receiving tens of millions of dollars in actual ransom payments made in the form of bitcoin.

CI's unique ability to follow the money trail continues to play an integral role in interdicting illicit financing activities and threats to our national security. These organizations cannot exist without the behind-the-scenes financial support funding their illicit activity. In November 2022, Mustafa Alowemer was sentenced to over 17 years in prison for his plan to bomb a church in Pittsburgh in the name of ISIS. Alowemer targeted the church, he described as a "Nigerian Christian" church, to "take revenge for our [ISIS] brothers in Nigeria." In April 2023, Dr. Charles Lieber, was sentenced for lying to federal authorities about his affiliation with the People's Republic of China's Thousand Talents Program and failing to report the associated income he received from the Wuhan University of Technology (WUT) in China.

CI also continued to share our best practices by hosting training sessions for other investigative agencies around the world. Most recently, in September 2023, CI trained investigators from Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates on techniques for identifying and combating the flow of money to and within terrorist organizations. Through our participation in The National Joint Terrorism Task Force (NJTTF) and The National Counterintelligence Task Force (NCITTF), CI and our agency partners stand ready in our shared missions to ensure the integrity of the U.S. financial system by combatting illicit finance.

CI targets money trails tied to transnational criminal organizations, which are often linked to a variety of crimes, including narcotics trafficking, terrorist financing, fraud, and illegal firearms distribution. CI also partners with other law enforcement agencies to pool resources to disrupt the transnational criminal organizations. CI holds key positions with the Executive Office and Fusion Center for the Organized Crime Drug Enforcement Task Force (OCDETF), the Financial Crimes Enforcement Network, the High Intensity Drug Trafficking Areas Task Force, and more. In fiscal year 2023, over 11% of CI's direct investigative time was dedicated to narcotics investigations.

In the last 10 years, CI was involved in approximately 36% of all OCDETF investigations and historically participated in 90% of all money laundering prosecutions across the United States. These investigations resulted in the removal of illegal weapons and drugs, including fentanyl, out of public circulation. In January 2023, Chance Alan Wilson, leader of the Universal Aryan Brotherhood (UAB), was sentenced to additional prison time after being found guilty of distribution of hundreds of kilograms of methamphetamine and other drugs. In total, 69 individuals associated with the UAB's operations have been charged and convicted in both state and federal court. Collectively, the individuals charged federally have been sentenced to 418 years in prison.

CI is not only focused on illegal drugs but also the misuse of prescription drugs. In June 2023, Dr. Dzung Ahn Pham was sentenced to over 12 years in federal prison for illegally distributing opioids and other powerful narcotics by writing prescriptions for patients without a legitimate medical purpose. Pham admitted he wrote prescriptions for approximately 53,693 pills of oxycodone, 68,795 pills of hydrocodone, and 29,286 pills of amphetamine salts.

CI's specialized financial expertise provides prosecutors with options for charging criminal co-conspirators, especially those who develop elaborate schemes to launder illicit funds via Black-Market Currency Exchanges (BMCE), Trade Based Money Laundering (TBML) schemes, licensed Money Service Businesses (MSB), Hawala transactions, shell/shelf corporations, casinos, smurfing, micro-structuring, bulk cash smuggling, or virtual currency exchanges. Miguel Salinas Salcedo served as a Mexico-based "peso broker," who arranged with drug traffickers to trade pesos that he controlled with drug traffickers to trade pesos that he controlled in Mexico for the cash proceeds in the United States. Salinas Salcedo and associates picked up the cash in the United States, deposited it into various bank accounts, and then made corresponding quantities of pesos available to the traffickers in Mexico. In August 2023, Salinas Salcedo was sentenced to eight years in prison for laundering drug proceeds.

In total, 69 individuals associated with the UAB's operations have been charged and convicted in both state and federal court. Collectively, the individuals charged federally have been sentenced to 418 years in prison.

CI is not only focused on illegal drugs but also the misuse of prescription drugs. In June 2023, Dr. Dzung Ahn Pham was sentenced to over 12 years in federal prison for illegally distributing opioids and other powerful narcotics by writing prescriptions for patients without a legitimate medical purpose. Pham admitted he wrote prescriptions for approximately 53,693 pills of oxycodone, 68,795 pills of hydrocodone, and 29,286 pills of amphetamine salts.

CI’s specialized financial expertise provides prosecutors with options for charging criminal co-conspirators, especially those who develop elaborate schemes to launder illicit funds via Black-Market Currency Exchanges (BMCE), Trade Based Money Laundering (TBML) schemes, licensed Money Service Businesses (MSB), Hawala transactions, shell/shelf corporations, casinos, smurfing, micro-structuring, bulk cash smuggling, or virtual currency exchanges. Miguel Salinas Salcedo served as a Mexico-based “peso broker,” who arranged with drug traffickers to trade pesos that he controlled in Mexico for the cash proceeds in the United States. Salinas Salcedo and associates picked up the cash in the United States, deposited it into various bank accounts, and then made corresponding quantities of pesos available to the traffickers in Mexico. In August 2023, Salinas Salcedo was sentenced to eight years in prison for laundering drug proceeds.
As our world becomes increasingly interconnected through global commerce and technology, CI serves as a leader in protecting the interests of the United States and its allies beyond the physical borders of our country. CI has encountered more complicated transnational crime conspiracies affecting all of CI’s investigative priorities, including core mission tax crimes, narcotics-related crimes, and other financial crimes. These schemes include tax evasion, international money laundering, illicit use of virtual currency, cyber hacking, terrorist financing, public corruption, human trafficking, and sanctions evasion.

To combat these offenses, CI has attachés posted in 11 overseas locations, who work with foreign governments and build partnerships to further financial crime investigations. In June 2023, CI deployed four cyber attachés on long-term details to Germany, Colombia, Singapore, and Australia to work with foreign governments on cyber investigations.

CI is a proud member of the Joint Chiefs of Global Tax Enforcement (J5), which attacks transnational tax crime by collaborating on enforcement operations, gathering information, sharing intelligence, and conducting coordinated operations against international criminals. The J5 includes the Australian Taxation Office, the Canada Revenue Agency, the Dutch Fiscal Information and Investigation Service, His Majesty’s Revenue and Customs, and CI. In July 2023, J5 efforts resulted in the indictment of an international tax advisor accused of concealing millions of dollars of income for high income Americans.

CI’s International Training Team (ITT) delivers trainings to representatives from multiple countries across the globe. Training provides foreign governments in developing nations with necessary tools to combat financial crimes. During fiscal year 2023, ITT taught 33 courses to over 1,100 law enforcement officials from 96 countries. In May 2023, CI delivered blockchain analysis tools and cyber training to Ukrainian law enforcement agencies. In September 2023, CI teamed up with the UK and the Netherlands to provide a second round of training, which was focused on cryptocurrency and blockchain tracing, to Ukrainian law enforcement officers.

CI participates on multiple national taskforces that are uniquely positioned to combat global threats. CI partners with the Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) to identify, develop, and add new individuals and entities to the Special Designated Nationals list. CI also plays an important role in sanctions enforcement. The agency plays an integral role in Taskforce KleptoCapture, which focuses on Russian sanction evaders.

Working globally to ensure criminals cannot seek cover overseas, CI tirelessly battles complex international financial crimes.

While CI is laser-focused on combatting financial crimes, CI also engages in community outreach to proactively protect fellow citizens from fraud, provide a helping hand, and assist when disaster strikes.

CI participates in hundreds of outreach events year-round to warn the public of fraud and scams, in addition to providing tips during tax filing season. CI offices participate in community events, such as National Night Out and the Law Enforcement Torch Run for Special Olympics. In our local communities, CI employees visited schools to encourage students to strive and thrive as future community leaders and to pursue education. CI offices throughout the country volunteered with a wide variety of organizations to help build homes, feed the hungry, and pack hygiene products and toiletries for those most in need.

CI is proud to partner with the Federal Emergency Management Agency (FEMA) to assist in natural disasters. FEMA designated 14 Emergency Management Functions (EMFs) to assist in disaster recovery efforts, which range from transportation to external affairs. CI has approximately 140 special agents assigned to the ESF #13 Cadre, who provide public safety and security assistance during natural disasters. During deployment, CI special agents provide security for aid centers, search and rescue teams, or field hospitals in the most impacted areas. In 2023, CI’s ESF#13 members were deployed to Maui, Hawaii following the devastating wildfires and to areas of Florida devastated by Hurricane Ian.

CI special agents play an important role in the Continuity of Operations (COOP) for IRS and Treasury, as they must evacuate executive leadership and provide security for the command center during emergency events. They are also the first responders in case of active shooter situations in many IRS buildings throughout the country.

CI employees also live and volunteer in the communities they work in, and they always step up to help those in need. This is exemplified by the actions taken in March 2023 by a special agent in New York. While getting ready for work, the special agent heard screaming and subsequent gunfire. Armed with his firearm and badge, the special agent ran outside to respond, finding a suspect had shot someone and then entered a taxi. The special agent held the man and taxi at gunpoint until responding NYPD officers could take the man into custody. CI special agents can always be counted on to answer when duty calls.

CI special agents also live and volunteer in the communities they work in, and they always step up to help those in need. This is exemplified by the actions taken in March 2023 by a special agent in New York. While getting ready for work, the special agent heard screaming and subsequent gunfire. Armed with his firearm and badge, the special agent ran outside to respond, finding a suspect had shot someone and then entered a taxi. The special agent held the man and taxi at gunpoint until responding NYPD officers could take the man into custody. CI special agents can always be counted on to answer when duty calls.
The defendants claimed that a close relative of the victim was in extreme danger, thereby inducing the victim to send thousands of dollars to help. In February 2023, Ejino Efiekerha was sentenced to over 7 years in federal prison for laundering the proceeds tied to grandchild-in-jail, inheritance, lottery and romance schemes.

CI also participated on 20 Transnational Elder Fraud Strike Forces, worked through the U.S. Department of Justice (DOJ): These Strike forces provide dedicated resources to identify the most harmful elder fraud schemes and to bring perpetrators to justice. Last fall, CI joined the DOJ in announcing the return of approximately $40 million in funds forfeited to the United States from the Western Union Company to nearly 25,000 victims, some of whom had fallen prey to elderly scams.

Raising awareness through education is a key component to CI’s effort to combat elder fraud. CI partnered with the private industry in outreach efforts to arm seniors with tips and resources to provide a critical first line of defense. In support of 2023 National Consumer Protection Week, CI published tips specifically geared to seniors, which were distributed to senior care facilities. The agency has also communicated information about elder fraud at various outreach events and has partnered with congressional representatives to educate seniors in their respective districts.

During the COVID-19 pandemic, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act that provided economic assistance to the American industry, including workers, families, and small businesses. The CARES Act authorized the Paycheck Protection Program (PPP) and Economic Injury Disaster Loans (EIDL) to help businesses survive the economic downturn caused by the pandemic. Unfortunately, criminals saw the CARES Act as an opportunity to defraud the government by submitting false claims.

CI has worked tirelessly finding and holding accountable individuals who defrauded these programs, dedicating over 10% of Direct Investigative Time (DIT) to combat CARES Act violations. Investigations range from fraudulently obtained employee refund tax credits to falsified PPP loans. PPP loans put in place with the intention of protecting employees have been exploited by fraudsters. As of September 30, 2023, CI investigated 1,444 tax and money laundering cases related to COVID-19 fraud, with an estimated fraud loss of $8.8 billion. Numerous investigations have resulted in lengthy prison sentences. Don Cisternino was sentenced to over eight years in federal prison for wire fraud, aggravated identity theft, and illegal monetary transactions for his scheme to obtain false PPP loans. Cisternino received more than $7.2 million in emergency funds through fraudulent PPP loans. Rather than use the funds to pay employees and business expenses, he purchased vehicles, including a Maserati and a Mercedes-Benz, and a 12,579 sq. ft. residence on a 12-acre estate. Once Cisternino caught wind of the investigation, he fled to Switzerland, but he was later extradited from Croatia to face charges.

The Employee Retention Credit (ERC) is a refundable tax credit for businesses who paid employees while shutdown due to the COVID-19 pandemic or for those who had significant declines in gross receipts from March 13, 2020 to December 31, 2021. The ERC was designed to encourage businesses to keep employees on their payroll. However, unscrupulous promoters have been encouraging businesses who do not qualify for the credit to file fraudulent ERC claims. As of September 30, 2023, CI has initiated 301 investigations involving over $3.4 billion of potentially fraudulent ERC claims for tax years 2020 through 2023.

CI’s commitment to finding COVID-19 fraud remains unwavering. Working closely with our law enforcement partners on the COVID-19 Fraud Enforcement Task Force, CI continues to bring criminals who defrauded these vital programs to justice.
CI is uniquely qualified to investigate corruption of all types, because, at its core, corruption is a crime of greed. Corruption is the abuse of power for personal gain. CI investigates elected individuals who violate the public’s trust. These individuals may be from all levels of government, including local, county, state, and federal government, as well as foreign entities. Corruption investigations may involve crimes, such as bribery, extortion, embezzlement, kickbacks, tax fraud, and money laundering.

A bribery scheme turned into nearly five years of jail time for Luis Arroyo, a former Illinois state representative who accepted thousands of dollars in bribes from a gaming company. In exchange for those bribes, Arroyo promoted legislation in the Illinois House of Representatives related to the sweepstakes industry and advised other state lawmakers to support the legislation.

Kickbacks, while unethical and unlawful, are also taxable. Kickback schemes run the gamut and can include payments in return for loan approvals, awarding lucrative contracts to personal associates, and pushing unnecessary medical procedures. In July 2023, Jimmy and Ashley Collins, a husband and wife, pleaded guilty to receiving kickback payments of over $45 million related to a $65 million TRICARE scheme. Their clinics were divested over 4,000 prescriptions and billed TRICARE for them. The prescriptions were diverted to a pharmacy, who then kicked back a percentage of the TRICARE reimbursement to the pair.

At times, corruption involves violations of the Foreign Corrupt Practices Act of 1977 (FCPA). FCPA prohibits certain individuals and entities from making payments to foreign government officials to obtain or retain business. In September 2023, Albemarle Corporation, a publicly traded specialty chemicals manufacturing company, paid a hefty price for FCPA violations. The company’s third-party sales agents and subsidiary employees conspired to pay bribes to government officials to obtain and retain chemical catalyst business with state-owned oil refineries in Vietnam, Indonesia, and India. A CI investigation into the arrangement resulted in the company agreeing to pay $218 million as part of a non-prosecution agreement.

While CI works diligently to put criminals out of business, we also recognize the hardships endured by crime victims. CI’s asset recovery program utilizes forfeiture authority to disrupt and dismantle criminal enterprises. Investigative seizures and forfeitures enable CI to not only seize assets and proceeds of criminal activity but also to help reimburse victims for their losses.

In the investigation of the Silk Road hacker, James Zhong, the government seized bitcoin valued at over $3.4 billion at the time of seizure. Using a decentralized bitcoin mixer, an overseas cryptocurrency exchange, and a variety of technology tools, Zhong stole 50,000 bitcoin from Silk Road, an online darknet marketplace. Due to CI’s ability to follow the money, even through the Dark web, special agents discovered and recovered the bitcoin stolen by Zhong.

Once adjudicated in federal court, the seized funds are forfeited to the Treasury Forfeiture Fund (TFF), which is managed by the Treasury Executive Office for Asset Forfeiture. Whenever possible, forfeited funds are returned to identified victims of the criminal activity. During fiscal year 2023, CI seized assets valued at approximately $272 million and forfeited approximately $3.5 billion in ill-gotten proceeds. In addition, approximately $30.3 million was refunded as part of CI’s asset recovery efforts.

If forfeited funds exceed the amount necessary to compensate victims of a crime or those with rightful claim to the asset, the proceeds are used to reimburse law enforcement agencies for expenses like enhanced training, equipment, and costs associated with conducting criminal investigations. In addition, the TFF shares a portion of forfeited funds with other federal, state, and local law enforcement agencies.
In addition to our tax and money laundering authorities, CI also investigates violations of The Bank Secrecy Act (BSA). The BSA mandates the disclosure of foreign bank accounts, the reporting of certain currency transactions conducted with businesses or financial institutions, and transportation of currency across U.S. borders. While the Financial Crimes Enforcement Network (FinCEN) is tasked with administering the BSA, the U.S. Treasury Secretary delegated responsibility for all criminal enforcement of the BSA to CI.

CI's BSA program has grown substantially since its inception in early 2000. BSA data helps investigators detect suspicious financial activity and identify unusual transactional patterns indicative of criminal behavior. CI leverages our data analytics to identify the highest quality leads for possible investigation. In fiscal year 2023, BSA data was queried in over 89.6% of CI investigations, and 14% of CI's investigations were initiated based on BSA information.

CI-led SAR Review Teams (SAR RTs) and Financial Crimes Task Forces (FCTFs) are in 92 federal judicial districts, where more than 200 special agents and investigative analysts collaborate with federal, state, and local law enforcement partners to identify and investigate financial crimes specific to their geographic areas. These crimes include tax, BSA violations, money laundering, narcotics, and more.

Chief Jim Lee described CI's valued role in the BSA program: “The Bank Secrecy Act exists to prevent financial institutions from being used as a vehicle by criminals to conceal or launder their ill-gotten gains. It also serves as a safety net for crime victims. Hundreds of millions of dollars in restitution have been awarded to crime victims because our agents were able to use BSA data to prove a crime was committed.” CI is the only federal law enforcement agency to win a FinCEN award in every award period since the program’s inception in 2015.

CI employs every lawful technique at our disposal, including undercover operations, to detect and investigate potential criminal violations within our jurisdiction, including businesses that willfully fail to file required disclosures under BSA. CI's undercover agents utilize sophisticated techniques to initiate contact with individuals perpetrating crimes and to gather the evidence necessary for prosecution.

In August 2023, Junaid “Jay” Sahibzada pleaded guilty to evading federal reporting requirements for businesses that conduct cash transactions above $10,000, by failing to file Form 8300. An undercover agent posing as a heroin dealer met with Sahibzada to discuss laundering drug proceeds through jewelry purchases. Sahibzada agreed to help conceal the purchases from the government by not filing the required Form 8300. Sahibzada later admitted to special agents that he had never filed Forms 8300, despite having completed multiple jewelry cash transactions exceeding $10,000.

BSA data is a force multiplier for CI's investigations and is crucial in combatting a wide variety of financial crimes, including tax evasion. In September 2023, Mark Gyetvay was sentenced to more than seven years in federal prison in a scheme to hide millions of dollars of income in undisclosed Swiss bank accounts. Gyetvay was convicted of failing to file a Report of Foreign Bank and Financial Accounts (FBAR), making a false statement to the IRS, and willfully failing to file tax returns.

The Bank Secrecy Act (BSA) data is a force multiplier for CI’s investigations and is crucial in combatting a wide variety of financial crimes, including tax evasion.”
FIELD OFFICE MAP
Click on an area name to go to that Field Office area.
WESTERN AREA

Click on a city to go to that Field Office or on an area name to go to that Field Office area.
Puerto Rico
U.S. Virgin Islands
Guam
DETROIT
CHICAGO
CINCINNATI
PHILADELPHIA
BOSTON
NEW YORK
NEWARK

NORTHERN AREA
Click on a city to go to that Field Office or on an area name to go to that Field Office area.

WESTERN AREA

SOUTHERN AREA
SOUTHERN AREA
Click on a city to go to that Field Office or on an area name to go to that Field Office area.

WESTERN AREA

NORTHERN AREA

Puerto Rico
U.S. Virgin Islands
Guam