ANNUAL REPORT 2025

IRS-CI

Table of Contents

Follow Us

For more information and to stay updated on IRS-CI:

@IRS_CI

IRS Criminal Investigation

IRS-CI

irs.gov/ci

Joint Chiefs of Global Tax Enforcement (J5)

J5 Website

View our interactive Annual Report.

IRS-CI

NAVIGATION MENU

Table of Contents • 2025 Snapshot • Field Office Map • Appendix

Message from the Chief

Each fiscal year, this report highlights not only our most significant cases and the resulting statistics, but also the dedication, sacrifice and professionalism of the IRS Criminal Investigation (IRS-CI) workforce. Our special agents and professional staff continue to demonstrate resilience, integrity and innovation as financial crimes grow more complex and demanding. None of our achievements as an agency would be possible without the people who work here at IRS-CI, and I am deeply grateful for their commitment to our mission.

In fiscal year 2025 (FY25), IRS-CI held some of the most egregious tax criminals accountable, dismantled schemes that targeted the vulnerable and defrauded government programs, applied its financial expertise to disrupt drug traffickers, and safeguarded our nation's national security by investigating sanctions evasion and illegal hiring schemes. Advanced data analytics, digital tools, and intelligence-sharing have become more integral than ever in uncovering patterns and anomalies indicative of criminal activity. As criminals become more sophisticated, our investigative techniques continue to evolve to keep pace.

Collaboration has been a cornerstone of our success. Initiatives such as CI-FIRST (Feedback in Response to Strategic Threats) strengthened our partnerships with financial institutions, enhancing communication and modernizing legal processes. This partnership redefines how we detect, disrupt and dismantle criminal networks. Internationally, our work with the Joint Chiefs of Global Tax Enforcement (J5) yielded tangible results, including cross-border investigations and intelligence-sharing that led to successful prosecutions. Through the J5, we published a series of reports highlighting fraud trends and typologies and saw our intelligence-sharing result in the guilty plea of a government contractor for evading millions of dollars in U.S. taxes and the conviction of the head of a cryptocurrency investment scheme for defrauding investors of millions. Domestically, our partnerships through the newly established Homeland Security Task Forces have reinforced our ability to support whole-of-government efforts that protect our communities and uphold the rule of law.

Starting in August, our special agents and professional staff began supporting Operation Safe and Beautiful in Washington, D.C., and in September, we began assisting the Restoring Law and Order in Memphis taskforce. These efforts bring together special agents from across the country to support local and federal law enforcement initiatives. While such missions extend beyond traditional tax enforcement, they demonstrate the adaptability of our agents and the broad value we bring to interagency efforts. These initiatives, though resource-intensive, underscore the trust placed in IRS-CI to deliver results wherever financial crimes intersect with broader national priorities.

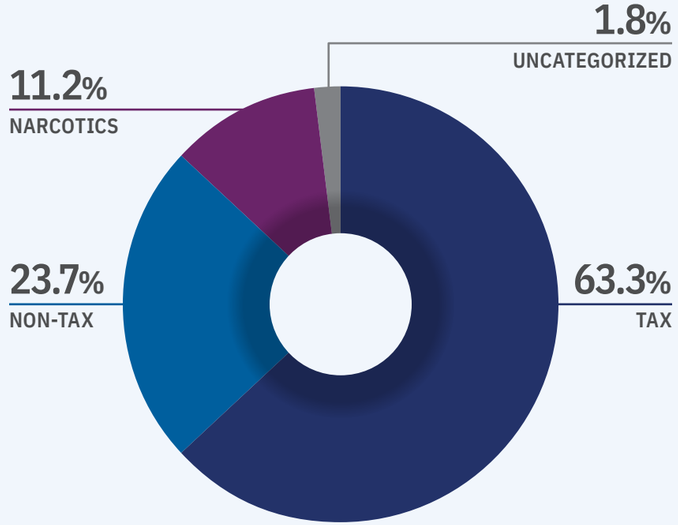
As we look forward, IRS-CI remains focused on combating threats to our tax and financial systems and protecting U.S. taxpayers. Our mission has not wavered, and I am confident that our team will continue to deliver results and meet the challenges of tomorrow.

Sincerely,

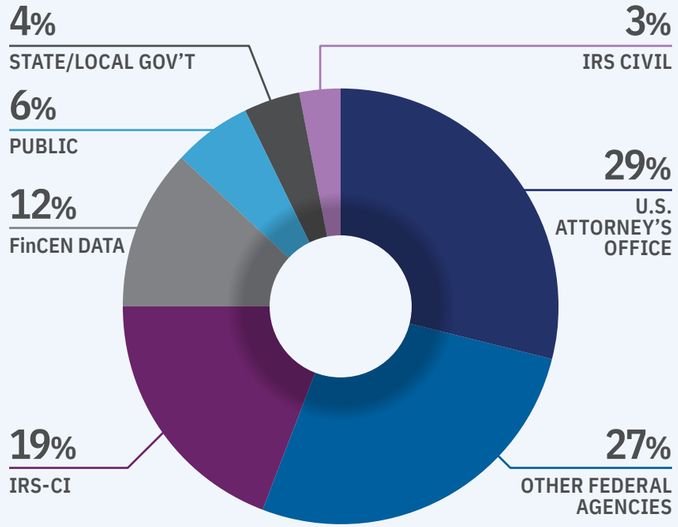
Guy Ficco
Chief, IRS Criminal Investigation

2025 Snapshot

Direct Investigative Time Spent



Investigation Sources



$4.49B
TAX FRAUD IDENTIFIED

$6.10B
OTHER IDENTIFIED FINANCIAL CRIMES

1445
WARRANTS EXECUTED

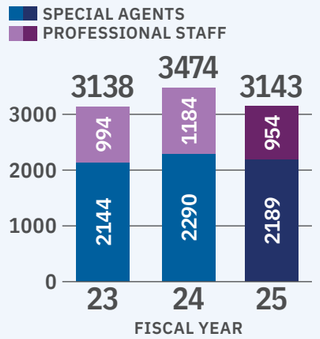
2043
REFERRED FOR PROSECUTION

89%
CONVICTION RATE

1611
CONVICTIONS

2.35
PETABYTES OF DIGITAL DATA

Staffing*



*Staffing levels are reported by fiscal year and reflect an actual count of employees based on employee master database as of PP19, and are adjusted for DRP/VERA separations.

IRS-CI's FY25 Global Impact (1/2)

IRS Criminal Investigation (IRS-CI), the law enforcement arm of the IRS, is the only federal agency with the authority to investigate potential criminal violations of the Internal Revenue Code. While the enforcement of U.S. tax laws remains our core priority, IRS-CI plays a critical role in satisfying broader national law enforcement priorities, including protecting national security and combating narcotics trafficking, terrorist financing, sanction violations, and cybercrimes. As a result of IRS-CI investigations, criminals may receive prison sentences for threatening America's financial and physical wellbeing. IRS-CI's enforcement efforts deter financial crimes by reinforcing trust in the U.S. financial system and strengthening the economy.

Founded in 1919 as the Intelligence Unit of the Department of Revenue, led by Chief Elmer Irey, the agency began with just six special agents. Today, IRS-CI consists of roughly 2,000 special agents who are sworn federal law enforcement officers that investigate the most complex criminal tax cases and a myriad of financial crimes. IRS-CI special agents are located in all 50 states, as well as Guam, Puerto Rico, and the Virgin Islands. IRS-CI also maintains 14 attaché posts abroad with a staff of approximately 30 attachés, deputy attachés, and investigative support staff.

IRS-CI also employs more than 1,000 professional staff who provide essential expertise and support to the agency's mission. These professionals analyze intelligence, conduct research, manage operations and deliver scientific and digital forensic analyses. Together, our special agents and professional staff continue to safeguard the integrity of our nation's tax and financial system.

In FY25, IRS-CI identified almost $4.5 billion in tax fraud and over $6 billion in fraud linked to other financial crimes. We referred 2,043 cases for prosecution, saw 1,611 convictions, and had a conviction rate of 89%, one of the highest in federal law enforcement.

While FY25 was a year that required our professionals across the agency to adapt to shifting priorities, we saw a significant increase in the amount of tax fraud identified — more than double the amount uncovered in FY24. Additionally, there was a 25% increase in the number of warrants executed throughout the year, along with an almost 14% rise in cases referred for prosecution. These accomplishments reflect our unwavering dedication to the mission of protecting the integrity of the tax system and ensuring fairness for all taxpayers.

Attaché Posts Abroad

BRANCH A:	BRANCH B:
Ottawa	Mexico City
London	Panama City
The Hague	The Bahamas
Frankfurt	Bogota
Dubai	Barbados
Canberra	Singapore
Sydney	Hong Kong

Expanding Federal Law Enforcement Partnerships

In FY25, IRS Criminal Investigation strengthened and expanded its federal law enforcement partnerships to address emerging national threats. Through newly established Homeland Security Task Forces, support to U.S. Immigration and Customs Enforcement for immigration enforcement, and participation in Operation Safe and Beautiful in Washington, D.C., and Restoring Law and Order in Memphis, IRS-CI deployed special agents nationwide to assist in combating violent crime, transnational organizations, and financial exploitation. These collaborations showcase the adaptability and expertise of IRS-CI's workforce in applying financial intelligence to complex, multi-agency operations. While extending beyond traditional tax enforcement, these efforts reinforce IRS-CI's vital role in protecting the nation's financial and public safety interests.

Money Laundering

1153 INVESTIGATIONS INITIATED

2313 SEIZURES

994 FORFEITURES

Narcotics and National Security

IRS-CI is well-known for solving some of the most complex financial crimes in our country. In 1931, the investigation of Alfonse "Al" Capone led to his indictment on federal income tax evasion. He was sentenced to 11 years in prison and ordered to pay a $50,000 fine and restitution of $215,000. Since then, IRS-CI has continued to play a crucial role in making the United States safer. Our agents identify transnational criminal organizations by targeting associated money trails, often linking the criminal organizations to crimes like narcotics trafficking, terrorist financing, illegal firearms distribution, and other fraud.

In FY25, and in accordance with the Executive Order *Protecting the American People Against Invasion*, the National Security Council directed the creation of Homeland Security Task Forces (HSTF). Co-led by Homeland Security Investigations and the FBI, HSTFs target criminal cartels, foreign gangs, and transnational criminal organizations throughout the United States. They investigate drug trafficking, money laundering, weapons trafficking, human trafficking, alien smuggling, homicide, extortion, kidnapping, and weapons trafficking. IRS-CI is a critical partner in this effort, and roughly 190 of our special agents sit on these taskforces across the country.

In FY25, IRS-CI special agents spent approximately 23.7% of their time investigating non-tax violations, initiated 1,412 cases, and referred 1,209 individuals for prosecution to the Department of Justice for non-tax violations.

In April 2025, Behrouz Parsarad, an Iranian national, was charged for his role in operating a dark web marketplace that served as a hub for illegal drugs and criminal cyber services, including stolen financial information, fraudulent identification documents, counterfeit currencies, and computer malware. According to the indictment, Parsarad launched Nemesis Market in March 2021. At its peak, the marketplace had over 150,000 users worldwide. Parsarad was charged with conspiracy to traffic drugs and money laundering conspiracy. In March 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions against Parsarad for his role as the administrator of Nemesis Market. According to OFAC, Nemesis Market facilitated the sale of nearly $30 million worth of drugs between 2021 and 2024.

NON-TAX CRIMES

1412 INVESTIGATIONS INITIATED

1209 PROSECUTIONS RECOMMENDED

1024 DEFENDANTS SENTENCED

IRS-CI's FY25 Global Impact (2/2)

Our efforts to combat terrorism and protect our national security also resulted in Christina Chapman, an Arizona woman, being sentenced to 8½ years in prison. She helped Information Technology (IT) workers located in North Korea steal the identities of U.S. nationals so they could apply for remote IT jobs and transmit false documents to the Department of Homeland Security. The scheme generated more than $17 million in illicit revenue for Chapman and North Korea. IRS-CI also participated in the investigation of Quanzhong An, who was an illegal agent for the People's Republic of China and led a harassment campaign against a U.S. resident and his family in an attempt to coerce the U.S. resident to return to China.

IRS-CI often plays a critical role in combatting drug trafficking due to our ability to trace financial records. In FY25, our team secured 447 convictions related to narcotics violations. In December 2024, Haiping Pan, a Chinese national, was sentenced to a decade in prison for laundering $62 million in illegal drug proceeds on behalf of traffickers in Mexico. IRS-CI assisted in an investigation where 11 defendants were sentenced to a combined 123 years in prison for operating a cartel-linked drug trafficking ring that smuggled nearly 400 pounds of methamphetamine and over 7 kilograms of fentanyl into the Midwest. IRS-CI's Detroit Field Office also assisted in a case where the judge, at sentencing, referred to the defendant, Jason Demyers, as a "kingpin" and sentenced him to 27 years in prison for his leadership of the multistate drug trafficking conspiracy.

National Law Enforcement Priorities

In May 2025, IRS-CI started providing support to U.S. Immigration and Customs Enforcement (ICE) with immigration enforcement efforts. IRS-CI dedicated special agents to assist ICE in facilitating arrest, detention, and deportation efforts, focusing on identifying transnational gang members and affiliates and locating children separated from their families after illegally entering the U.S.

As the only federal law enforcement agency with jurisdiction over income tax violations, IRS-CI is committed to investigating tax crimes related to fraudulent refund claims, legal and illegal income source tax evasion, and emerging trends in financial exploitation including employment tax violations. Our investigative priorities include rooting out fraud in government contracts, combating false claims to the IRS, and targeting schemes that prey on vulnerable individuals and compromise their financial security. Our Advanced Analytics and Innovation team continues to stay at the forefront of identifying new schemes and uncovering the methodology these criminals use to defraud their victims. We use the latest technology to refine our investigative approach to improve scheme detection and improve the efficiency of our data analytics and investigations.

One area where these investigative priorities and data-driven strategies have proven especially effective is in addressing employment tax fraud and payroll schemes that exploit vulnerable workers and undermine the tax system. Employers are required to deduct employment taxes from employees' wages and pay a portion of these taxes to the U.S. government. IRS-CI investigates large-scale payroll and worksite fraud schemes nationwide. A lot of these cases involve labor intensive industries, such as construction, agriculture, and hospitality. In certain instances, staffing companies or "labor brokers" pay workers off the books to evade taxes and hide unauthorized employment.

Manuel Domingos Pita, a Florida businessman, was sentenced to 48 months in prison and ordered to pay $55 million in restitution for employing migrant laborers illegally, evading payroll taxes, and causing a worker's death. In Oregon, David Katz was sentenced to four years in prison and ordered to repay nearly $45 million for a $177 million payroll tax evasion scheme. Katz conspired with others in the construction industry to facilitate "under-the-table" payments to construction workers. Four Honduran nationals were indicted in Florida for running an off-the-books payroll operation, and the owners of several Florida labor-staffing companies were sentenced for tax fraud, immigration violations, and laundering illicit proceeds.

IRS-CI continues to prioritize cybercrime investigations, recognizing that modern financial crimes increasingly rely on the internet, computer networks, and digital communication to expand their reach and complexity. These cases are often among the agency's largest, often resulting in lengthy prison terms, significant forfeitures, and seizures. In FY25 alone, IRS-CI saw 54 convictions in cyber-related investigations with an average sentencing of 63 months incarceration. In FY25, Oluwole Adegboruwa was sentenced to 30 years in prison for operating a multimillion-dollar dark web operation that distributed more than 300,000 oxycodone pills and laundered nearly $9.1 million in proceeds. Roman Sterlingov, a dual Russian-Swedish national, earned himself a 12½ year prison sentence for operating the darknet cryptocurrency mixer *Bitcoin Fog*. And Ilya Lichtenstein, who orchestrated a massive hack of the cryptocurrency exchange Bitfinex and then laundered nearly 120,000 stolen bitcoin, was sentenced to five years in prison. To meet the global nature of these crimes, IRS-CI used advanced analytics to identify data trends and staffing resources, including cybercrime units in Los Angeles and Washington, D.C., specialized attachés assigned to international posts, and partnerships around the world.

In March 2025, IRS-CI announced CI-FIRST (Feedback In Response to Strategic Threats), the agency's flagship initiative to modernize the way IRS-CI works with financial institutions. CI-FIRST addresses challenges in Bank Secrecy Act reporting by providing feedback to help banks understand what is most useful to investigators, while enhancing the speed and precision with which agents can identify, disrupt, and prosecute financial crime. The Optimizing Financial Records Requests (OFRR) initiative streamlines and standardizes how law enforcement agencies request and how financial institutions respond to legal order and subpoena requests.

IRS-CI hosted more than a dozen global financial institutions at its first executive forum in Washington, D.C. in August 2025, and hundreds of financial industry, regulatory agency, and law enforcement representatives attended regional forums in Tampa, Florida, and Los Angeles, California, in September 2025.

IRS-CI prioritizes financial fraud schemes targeting U.S. citizens and government programs. In FY25 we identified over $10.6 billion in financial fraud including tax and non-tax offenses. We continue to see lengthy prison sentences for fraud in connection with the COVID-19 pandemic. In a landmark sentence, Shafii Farah, one of the masterminds behind a COVID-19 fraud scheme, was sentenced to 28 years in prison for defrauding American taxpayers of over $250 million. Thus far, 73 defendants have been indicted for their participation in this scheme. In FY25, IRS-CI initiated 588 investigations involving more than $5.6 billion of potentially fraudulent ERCs related to tax years 2020, 2021, 2022, 2023, and 2024. Of these investigations, 108 have resulted in federal charges to date.

This year, our financial fraud investigations revealed recurring themes of long-running deception, abuse of trust, and massive financial harm to communities. Our investigators uncovered a $24.5 million Ponzi scheme, sweeping identity-theft frauds, and secured the conviction of former speaker of the Illinois House of Representatives, Michael Madigan, who was sentenced to seven years for using his official position for personal benefit. Whether siphoning government benefits, exploiting community ties, or misusing political power, each case underscores how fraud erodes confidence in institutions, communities, and public programs, reinforcing why IRS-CI remains central to protecting the integrity of the financial system.

TAX CRIMES

1380 INVESTIGATIONS INITIATED

834 PROSECUTIONS RECOMMENDED

589 DEFENDANTS SENTENCED

Significant Cases (1/3)

TD Bank Investigation

Newark Field Office

For almost a decade, TD Bank NA and its parent company, TD Bank US Holding Company, the 10th largest bank in the United States, had long-term, pervasive, and systemic deficiencies in its U.S. anti-money laundering (AML) policies, procedures, and controls but failed to take appropriate remedial action. Instead, senior executives at TD Bank enforced a budget mandate, referred to internally as a "flat cost paradigm," requiring that TD Bank's budget not increase year-over-year, despite its profits and risk profile increasing significantly over the same period. Although TD Bank maintained elements of an AML program that appeared adequate on paper, fundamental, widespread flaws in its AML program made TD Bank an "easy target" for perpetrators of financial crime.

TD Bank's federal regulators and their own internal audit staff repeatedly identified concerns about its transaction monitoring program, a key element of an effective AML program, which is necessary to detect and report suspicious activities and financial transactions. TD Bank intentionally did not automatically monitor all domestic automated clearinghouse transactions (ACH), most check activity, and numerous other transaction types, resulting in 92% of their total transaction volume going unmonitored from January 2018 through April 2024. This amounted to approximately $18.3 trillion of unmonitored transaction activity.

Employees of TD Bank described the institution as a "convenient" target for criminals, which allowed hundreds of millions of dollars to pass through the bank. The investigation revealed at least three distinct money laundering networks that collectively transferred more than $670 million through TD Bank accounts between 2019 and 2023. The Justice Department has charged over two dozen individuals across these schemes, including two bank insiders. TD Bank's plea agreement requires continued cooperation in ongoing investigations of individuals. In November 2024, TD Bank was ordered to forfeit over $452 million and to pay a criminal fine of $1.4 billion.

Global Export Control and Sanctions Evasion Scheme

New York Field Office

From 2019 through 2022, Vadim Yermolenko, a dual U.S. and Russian national residing in New Jersey, played a key role in a transnational procurement and money laundering network that illegally acquired U.S.-made dual-use electronics and military-grade ammunition intended for Russian military and intelligence entities.

Yermolenko was affiliated with Serniya Engineering (Serniya) and Sertal LLC (Sertal), two Moscow-based procurement companies that operated a network of shell companies and bank accounts throughout the world, including in the United States. These companies concealed involvement of the Russian government and end-users of highly sensitive electronic components, some which are used in the development of nuclear weapons or other military applications. Serniya, Sertal, and several individuals and companies involved in the scheme were placed on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals List in February 2022, which allows the U.S. to place sanctions on these entities.

Yermolenko helped set up shell companies and U.S. bank accounts to conceal the Russian government's involvement, funneling over $12 million through accounts he controlled. Yermolenko failed to report the funds to the IRS. These funds were used in part to purchase sensitive radar equipment for surveillance, military research, and development. Yermolenko pleaded guilty to conspiracy to violate the Export Control Reform Act, bank fraud conspiracy, and conspiracy to defraud the United States. He was sentenced to 30 months in prison and ordered to pay a forfeiture money judgment of $75,547.

Bitfinex Hack

Washington, D.C. Field Office

In 2016, Ilya Lichtenstein hacked into Bitfinex, a global cryptocurrency exchange, using advanced hacking tools and techniques. Once inside the network, Lichtenstein fraudulently authorized more than 2,000 transactions transferring 119,754 bitcoin from Bitfinex to a cryptocurrency wallet in his control. Lichtenstein then took steps to cover his tracks by deleting access credentials and other log files from Bitfinex's network that could have revealed his conduct to law enforcement. Following the hack, Lichtenstein enlisted the help of his wife, Heather Morgan, in laundering the stolen funds. At the time of the hack, the bitcoin was valued at $71 million.

Lichtenstein, at times with Morgan's assistance, employed numerous sophisticated laundering techniques that ranged from using fictitious identities to set up online accounts to utilizing computer programs to automate transactions to converting bitcoin to other forms of cryptocurrency in a practice known as chain hopping. He then used U.S.-based business accounts to legitimize his and Morgan's banking activity and exchanged a portion of the stolen funds for gold coins.

Lichtenstein and Morgan both pleaded guilty. Lichtenstein was sentenced to five years in prison, and Morgan was sentenced to 18 months. Several billion dollars of illicit proceeds have also been recovered through seizure and forfeiture due to the appreciation of the stolen funds.

North Korean Information Technology Scheme

Phoenix Field Office

From 2020 through 2023, Christina Chapman conspired with and assisted North Korean IT workers in a scheme that generated more than $17 million in illicit revenue for herself and North Korea. Using stolen and purchased identities of U.S. nationals, North Korean workers applied for remote IT jobs at over 300 U.S. companies, including Fortune 500 corporations, major television networks, American car makers, and tech companies.

Chapman operated a "laptop farm," where she received and hosted computers from U.S. companies at her home, leading the companies to believe these workers were in the United States. Chapman also shipped 49 laptops and other devices supplied by U.S. companies to locations overseas, including multiple shipments to a city in China near North Korea.

Much of the $17.1 million was falsely reported as wages to the IRS and Social Security Administration in the names of U.S. individuals whose identities had been stolen or borrowed. Chapman pleaded guilty to conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to launder monetary instruments. She was sentenced to 102 months in prison and ordered to forfeit $284,555.92 that she planned to pay to the North Koreans and pay a judgement of $176,850.

CYBERCRIMES

54 CONVICTIONS

63 Mos AVERAGE SENTENCING

$149M ASSETS SEIZED

Significant Cases (2/3)

Par Funding

Philadelphia Field Office

For almost a decade, Joseph LaForte, CEO of Complete Business Solutions Group Inc., dba Par Funding ("Par Funding"), orchestrated a large-scale fraud totaling approximately $404 million. LaForte marketed Par Funding as a high-yield lending opportunity, when it actually operated as a criminal enterprise. As the undisputed leader of the enterprise, he misled investors about the company's financial performance, concealed his prior felony convictions, and directed aggressive and sometimes violent collection tactics against borrowers.

LaForte and his co-conspirators, one of which was his brother, James LaForte, defrauded investors by providing false or misleading information about the company's performance, insurance coverage, and other important facts. Par Funding's principal means of generating income was to advance money to businesses (known as merchant cash advance or MCA customers) that needed short-term financing at high rates of return. They then engaged in threats of violence and extortion to collect overdue payments. Additionally, they lied about the financial position of the company.

Joseph LaForte caused Par Funding to pay him and his wife more than $120 million in fraudulent proceeds, which he used to purchase homes, vacation properties, vehicles, artwork, jewelry, dozens of investment properties, a boat, and a private jet. He committed a variety of tax crimes related to these fraudulent proceeds, including conspiracy to defraud the IRS and filing false income tax and employment tax returns. His tax crimes resulted in more than $8 million in losses to the IRS and $1.6 million in losses to the Pennsylvania Department of Revenue.

LaForte was convicted in numerous federal and state charges including RICO conspiracy, securities fraud, tax fraud, and obstruction of justice. He was sentenced to 186 months in prison and three years of supervised release, including one year of house arrest. LaForte was also ordered to pay restitution of $314 million and a $120 million money forfeiture judgment, and he was ordered to forfeit various assets, including a private jet and an investment account totaling approximately $20 million.

Bitwise Industries

Oakland Field Office

From 2022 through May of 2023, founders Jake Soberal and Irma Olguin Jr. engaged in a scheme to defraud investors of their company, Bitwise Industries. At the time, Bitwise was the largest startup company from California's Central Valley. The company's objective was to use technology to create jobs for underserved groups of people and to revitalize blighted urban areas, all while demonstrating profitability to investors. However, Soberal and Olguin fabricated investor materials, falsified audit reports, altered bank statements, and forged documents to portray Bitwise as profitable, when the company actually had minimal revenue and was running out of funds.

In a February 2022 presentation and a July 2022 prospectus, Olguin and Soberal represented to investors that Bitwise's cash balance was over $44 million, and their revenue was more than $58 million, when Bitwise had less than $12 million in cash, and the company's revenue was non-existent. They made similar representations in March 2023, when they overstated their cash balance by $72 million and claimed $143 million in revenues, while they were negligible.

Their deception caused nearly 1,000 employees and contractors to abruptly lose their jobs when the company collapsed in May 2023. Their actions had widespread economic and personal fallout, prompting serious sentencing enhancements due to their abuse of trust, professional status, and calculated efforts to conceal the fraud. Soberal and Olguin were convicted for conspiracy to commit wire fraud and wire fraud, sentenced to 11 and 9 years in prison, respectively, and were ordered to pay restitution to victims of over $114 million.

Feeding Our Future Fraud Scheme

Chicago Field Office

From April 2020 to January 2022, Abdiaziz Shafii Farah, a Minnesota businessman, played a leading role in a COVID-19 fraud scheme totaling over $300 million, one of the largest ever. Farah used his company, Empire Cuisine & Market, to enroll in the federal Child Nutrition Program (CHIP) during the COVID-19 pandemic, and he created over 30 sham distribution sites. Farah submitted falsified rosters and invoices to claim over 18 million meals for underprivileged children that were never served.

He ran a "pay-to-play" kickback system, bribing program employees to approve and sustain the scheme. He used the proceeds of this scheme to purchase luxury real estate, vehicles, jewelry, and overseas investments. He personally pocketed over $8 million from the scheme. Farah was convicted of conspiracy charges, false statements, bribery-related charges, and 11 counts of money laundering. He was sentenced to 28 years in prison followed by three years of supervised release, and he was ordered to pay restitution of $47.92 million.

At least 75 individuals have been charged in connection with this scheme. Mukhtar Mohamed Shariff, CEO of Afrique Hospitality Group, engaged in similar conduct and was sentenced to 210 months in prison followed by three years of supervised release. He was also ordered to pay almost $50 million in restitution. Sharon Denise Ross was sentenced to 43 months in prison and ordered to pay $2.4 million in restitution for claiming to have served thousands of children each day at the House of Refuge Twin Cities, a St. Paul based non-profit.

Credit Suisse Services AG

International Tax & Financial Crimes Group (Washington, D.C.)

Credit Suisse Services AG, (Credit Suisse) pleaded guilty for conspiring to help U.S. taxpayers hide more than $4 billion in at least 475 offshore accounts from the IRS. Between January 2010 and July 2021, Credit Suisse, who served high-net-worth clients globally, colluded with U.S. clients and employees to conceal asset ownership and income held at the bank. This enabled clients to evade U.S. tax obligations by opening undeclared offshore accounts, using private banking services to obscure assets from the IRS, and failing to file required Reports of Foreign Bank and Financial Accounts (FBARs). Bankers knowingly falsified records—including fictitious donation paperwork—and managed over $1 billion in undocumented accounts. This misconduct was in violation of a May 2014 plea agreement with the United States.

Credit Suisse also entered into a non-prosecution agreement (NPA) concerning its Singapore operations, where from 2014 to June 2023, it maintained undeclared U.S.-related accounts with assets exceeding $2 billion and failed to identify U.S. indicia or the true beneficial owners. The bank agreed to cooperate fully with DOJ investigations and committed to paying substantial monetary penalties.

As part of the resolution, the bank agreed to pay approximately $510.6 million in total penalties, restitution, forfeiture, and fines. UBS—Credit Suisse's parent since its 2023 acquisition—is required under the agreement to fully cooperate with ongoing investigations and disclose information regarding U.S.-related accounts.

ASSET FORFEITURES

$816M* SEIZURES
* Value at time of seizure

$508M FORFEITURES

$99M ASSET RECOVERY

Significant Cases (3/3)

Multi-State Drug Trafficking and Money Laundering

Tampa Field Office

From 2017 through 2023, a violent drug trafficking organization led by Dudzinski Edwinn Poole, known as “Zink,” distributed massive quantities of methamphetamine and fentanyl across multiple states, including Florida, Georgia, and Ohio. The organization relied on a network of couriers, stash houses, and mailed packages to move narcotics. They then laundered their proceeds, including through an entertainment business that disguised illicit revenue as legitimate income. The investigation uncovered a wide-reaching conspiracy involving suppliers, distributors, couriers, and financial operatives who played roles in sustaining the drug pipeline and concealing profits.

Investigators seized more than 250 pounds of methamphetamine and fentanyl, along with firearms, vehicles, jewelry, and residences purchased with the drug proceeds. Leaders used commercial flights and the mail to transport drugs, while laundering millions of dollars through shell operations and cash couriers. Evidence revealed that members of the organization used violence, threats, and intimidation to maintain control of their operation and profits.

Seventeen defendants were convicted, either through guilty pleas or jury trials. Sentences varied depending on the defendant’s role: Michael Chester was sentenced to life in prison, reflecting his leadership in the conspiracy, while Poole received 21 years and 10 months. Several others received terms ranging from six years to more than 30 years. The wide range of sentences highlights the differing levels of responsibility within the organization, from masterminds and major distributors to couriers and facilitators.

COVID-19 Pandemic Fraud Scheme

Los Angeles Field Office

From June 2020 through December 2021, Casie Hynes engaged in a wide-ranging fraud scheme exploiting COVID-19 relief programs and pandemic tax credits. Hynes submitted over 80 fraudulent loan applications through the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program, seeking more than $3.1 million in relief funds. She fabricated the number of employees, payroll amounts, and supporting tax and bank records, and she used the personal information and signatures of others without authorization. Through this scheme, she successfully obtained approximately $2.25 million in fraudulent loan proceeds.

In addition, between May 2021 and April 2022, Hynes submitted a dozen fraudulent tax filings claiming nearly $1.3 million in pandemic-related tax credits, including the Employee Retention Credit and Paid Sick and Family Leave Credits. These filings were submitted on behalf of companies she controlled, such as Nasty Womxn Project LLC, She Suite Ventures, and Casie Hynes Consulting, and were based on fictitious wages and employees. Although those tax credit claims were denied, the attempt underscored her use of multiple pandemic relief programs to maximize illicit gain.

Hynes was convicted of wire fraud and presenting false claims to the United States. She was sentenced to 60 months in prison and ordered to pay more than $2.37 million in restitution.

Syndicated Conservation Easements

Charlotte Field Office

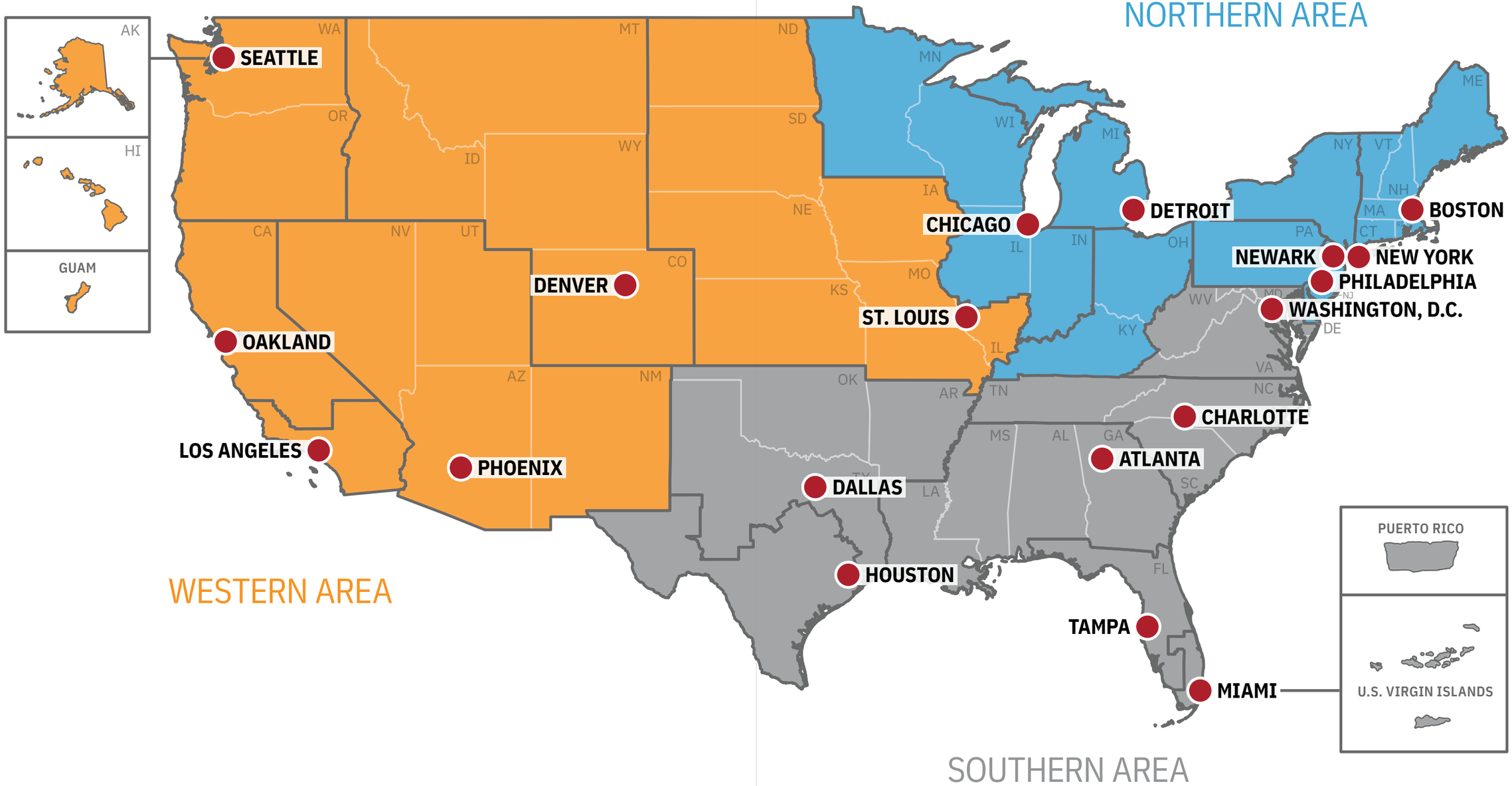
IRS-CI continues to investigate individuals associated with an abusive tax scheme tied to syndicated conservation easement transactions. From 2014 through at least 2019, Victor Smith, CPA, a founding partner of an Atlanta-based accounting firm, promoted and sold tax deductions to his wealthy clients in illegal syndicated conservation easement tax shelters, which were organized and created by co-defendants Jack Fisher, James Sinnott, and others. Smith and his firm sold approximately $14 million in false tax deductions to their clients, causing a tax loss to the IRS of about $4.8 million. Smith earned $491,400 in commissions.

William Tomasello, a CPA at another accounting firm, also promoted and sold units to his wealthy clients causing a tax loss of about $2.3 million. He earned approximately $525,072 in commissions.

Smith and Tomasello both knew that, contrary to law, these tax shelters lacked economic substance and that their wealthy clients participated in these sham investments only to obtain a tax deduction. For example, a client who purchased units in a partnership had to vote ostensibly on what to do with the partnership’s land. However, Smith and Tomasello knew that the vote held by the partnerships each year was just for optics, and the land invariably would be donated largely as a conservation easement. Smith and Tomasello also knowingly instructed and caused their clients to falsely backdate documents like subscription agreements and checks related to the illegal tax shelters. In October 2024, they were each sentenced to 20 months in prison for their role in the scheme.

In FY25, eight defendants were convicted of criminal conduct related to this scheme, which was orchestrated by Fisher and Sinnott. Fisher and Sinnott were convicted after trial and sentenced in 2024. Other defendants include appraiser Walter Douglas “Terry” Roberts, Ralph Anderson, and Vui Bui, an attorney and partner at Sinnott & Co. Bui was sentenced to 16 months in prison for his role in this scheme.

Field Office Map



Appendix (1/2)

This appendix includes investigation data appearing in the annual report as well as extended information regarding incarceration rates.

FY Combined Results

	2025	2024	2023
Investigations Initiated	2792	2667	2676
Prosecution Recommendations	2043	1794	1838
Informations/ Indictments	1726	1669	1676
Sentenced	1613	1582	1479
Incarceration Rate	76%	76%	79%
Average Months to Serve	49	44	48

Abusive Tax Schemes

	2025	2024	2023
Investigations Initiated	34	92	103
Prosecution Recommendations	17	55	36
Informations/ Indictments	18	37	40
Sentenced	30	36	26
Incarceration Rate	77%	83%	77%
Average Months to Serve	24	47	36

Abusive Return Preparer Program

	2025	2024	2023
Investigations Initiated	206	190	201
Prosecution Recommendations	169	91	108
Informations/ Indictments	92	83	92
Sentenced	83	84	134
Incarceration Rate	77%	80%	72%
Average Months to Serve	27	20	23

Bank Secrecy Act (BSA)

	2025	2024	2023
Investigations Initiated	541	542	511
Prosecution Recommendations	357	381	350
Informations/ Indictments	310	347	319
Sentenced	323	316	235
Incarceration Rate	81%	73%	77%
Average Months to Serve	34	29	32

Corporate Fraud

	2025	2024	2023
Investigations Initiated	37	23	34
Prosecution Recommendations	19	16	31
Informations/ Indictments	23	14	26
Sentenced	26	22	19
Incarceration Rate	50%	77%	79%
Average Months to Serve	25	44	22

Financial Institution Fraud

	2025	2024	2023
Investigations Initiated	52	32	28
Prosecution Recommendations	29	21	25
Informations/ Indictments	28	27	20
Sentenced	21	30	16
Incarceration Rate	76%	47%	81%
Average Months to Serve	40	18	45

Employment Tax

	2025	2024	2023
Investigations Initiated	205	209	221
Prosecution Recommendations	142	113	115
Informations/ Indictments	96	106	128
Sentenced	121	104	103
Incarceration Rate	82%	72%	84%
Average Months to Serve	22	17	20

Healthcare Fraud

	2025	2024	2023
Investigations Initiated	64	60	44
Prosecution Recommendations	33	36	36
Informations/ Indictments	34	34	32
Sentenced	59	58	56
Incarceration Rate	58%	62%	80%
Average Months to Serve	23	25	39

Appendix (2/2)

This appendix includes investigation data appearing in the annual report as well as extended information regarding incarceration rates.

Identity Theft

	2025	2024	2023
Investigations Initiated	161	106	137
Prosecution Recommendations	116	74	96
Informations/ Indictments	118	67	98
Sentenced	76	87	81
Incarceration Rate	87%	89%	80%
Average Months to Serve	63	58	50

Money Laundering

	2025	2024	2023
Investigations Initiated	1153	1080	955
Prosecution Recommendations	868	805	805
Informations/ Indictments	695	693	675
Sentenced	549	515	479
Incarceration Rate	86%	81%	84%
Average Months to Serve	75	67	74

International Operations

	2025	2024	2023
Investigations Initiated	142	174	147
Prosecution Recommendations	123	139	128
Informations/ Indictments	132	152	117
Sentenced	148	149	128
Incarceration Rate	81%	82%	85%
Average Months to Serve	66	59	63

Narcotics

	2025	2024	2023
Investigations Initiated	577	627	528
Prosecution Recommendations	505	523	480
Informations/ Indictments	452	514	451
Sentenced	489	468	418
Incarceration Rate	83%	82%	85%
Average Months to Serve	89	83	89

Non-Filer

	2025	2024	2023
Investigations Initiated	245	221	251
Prosecution Recommendations	147	131	141
Informations/ Indictments	118	127	115
Sentenced	126	101	116
Incarceration Rate	80%	75%	83%
Average Months to Serve	34	25	28

Questionable Refund Program

	2025	2024	2023
Investigations Initiated	127	109	93
Prosecution Recommendations	80	43	39
Informations/ Indictments	69	18	40
Sentenced	40	57	65
Incarceration Rate	78%	84%	72%
Average Months to Serve	32	52	42

Public Corruption

	2025	2024	2023
Investigations Initiated	32	44	37
Prosecution Recommendations	25	38	18
Informations/ Indictments	31	34	15
Sentenced	28	26	38
Incarceration Rate	79%	77%	82%
Average Months to Serve	51	32	37

Terrorism

	2025	2024	2023
Investigations Initiated	15	21	14
Prosecution Recommendations	8	15	12
Informations/ Indictments	9	15	12
Sentenced	10	28	9
Incarceration Rate	80%	57%	67%
Average Months to Serve	43	17	127

IRS-CI Organization Chart

Office of the Chief

- Office of Communication
- Commissioner's Protection Detail

Strategy

- National Criminal Investigation Training Academy
- Asset and Knowledge Management
- Assurance and Advisory
- Workforce Development
- Human Resources
- Finance
- Project Office

Cyber and Forensic Services

- Cybercrimes
- Digital Forensics
- Center for Science and Design

Advanced Analytics and Innovation

- Applied Analytics
- Nationally Coordinated Investigations Unit
- Systems and Operational Support
- Refund Fraud and Investigative Support
- Innovation
- Data Management & Governance

Technology Operations

- Development
- Field Operations

Global Operations

- Global Operations Policy & Support
- Asset Recovery and Investigative Services
- Financial Crimes
- Narcotics and National Security Section
- Special Investigative Techniques
- International Field Operations and International Liaison and Strategy

Field Operations

- Western Area Field Operations
- Northern Area Field Operations
- Southern Area Field Operations

IRS-CI

ANNUAL REPORT 2025

Publication 3583 (Rev. 12-2025) Catalog Number 29201R Department of the Treasury **Internal Revenue Service** www.irs.gov