

COVID-19 FRAUD ENFORCEMENT TASK FORCE 2024 REPORT

APRIL 2024



Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY



Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau



I. Executive Summary

The COVID-19 Fraud Enforcement Task Force (CFETF) is pleased to present in this 2024 report a compilation of its member agencies' accomplishments to date to combat pandemic fraud. While the CFETF has made significant progress to identify, investigate, and punish COVID-19 fraud, substantial work remains in the face of numerous challenges.

The CFETF's coordinated approach has resulted in:

- Over 3,500 defendants criminally charged
- Over 400 civil settlements and judgments
- Over \$1.4 billion in fraudulently obtained CARES Act funds seized or forfeited
- A new, integrated, and data-driven approach to investigate government program fraud

To continue the CFETF's work and ensure COVID-19 fraudsters don't get away with it, legislation is required to:

- Extend the statute of limitations for all COVID-19 fraud-related offenses
- Extend the PRAC's statutory authorization
- Adequately resource COVID-19 fraud data sharing, lead development, investigations, prosecutions, and asset recoveries

The COVID-19 pandemic prompted the United States government to establish and administer federal relief programs at a size and scope virtually unprecedented in our nation's history. And while these relief programs helped to mitigate some of the pandemic's most devastating effects, they also came with a cost. As has become increasingly clear in the months and years

since the pandemic's peak, many of these programs were targeted by fraudsters and other criminals who sought to exploit the government's relief efforts for their personal gain.

The Department of Justice has worked closely with its law enforcement partners, including multiple Offices of Inspectors General, to mobilize a coordinated response to these illegal acts. The Attorney General established the CFETF in 2021, subsequently creating the position of Director of COVID-19 Fraud Enforcement and launching the COVID-19 Fraud Enforcement Strike Forces.

This coordinated approach has led to enforcement successes, including criminal charges against more than 3,500 defendants, civil enforcement actions resulting in more than 400 civil settlements and judgments, and more than \$1.4 billion in seizures and forfeitures. In doing so, the CFETF has disrupted transnational criminal networks and domestic violent offenders, making communities safer here and abroad. Importantly, the CFETF has leveraged its interagency network to make strategic improvements in how the government investigates fraud, using the wide array of skills from its members to devise more effective fraud fighting tactics.

While this report highlights these accomplishments, much work remains in the fight against COVID-19 fraud. CFETF members have seen their budgets cut, straining resources to develop investigations and prosecute offenders. The first years of the pandemic fraud response were dedicated to coordination, data collection, and the establishment of interagency data sharing to generate actionable leads.

But challenges loom. Four years have passed since the pandemic began. In the coming years, investigative targets will increasingly argue that their conduct falls outside the statute of limitations, threatening prosecutors' ability to hold wrongdoers accountable. The Pandemic Response Accountability Committee (PRAC), a body of 20 federal Inspectors General overseeing pandemic relief spending, is due to sunset next year. And tightening budgets across the federal government make it increasingly difficult to adequately resource CFETF's essential work. But to address these issues, legislation is required.

The time to act is now. Under current CFETF funding levels, the government lacks sufficient resources to prosecute fraudsters who didn't just commit pandemic fraud, but targeted the elderly through romance fraud schemes, U.S. companies through business email compromise (BEC) schemes, and government programs through unemployment insurance fraud. DOJ prosecutors in Baltimore and Detroit have even taken down gang members and violent criminals for pandemic fraud, securing prison sentences and recovering weapons and narcotics.

If we fail to provide the necessary PRAC data to CFETF agencies or neglect to extend the statute of limitations, our agents and prosecutors won't be able to

finish the job—losing the opportunity to recoup hundreds of millions of dollars in fraud proceeds and placing our citizens and government institutions at risk of future criminal victimization.

The CFETF and its member agencies have ongoing investigations into hundreds of identity thieves, transnational fraud and money laundering networks, large-dollar individual fraudsters, and the businesses that facilitated these crimes. Government employees who chose to fraudulently obtain pandemic benefits are also being investigated. Civil enforcement tools are being utilized to recover misappropriated funds from businesses and individuals throughout the country. CFETF member agencies have improved their data analytics capabilities and are using these new skills to investigate fraud more efficiently and effectively. And the lessons learned by law enforcement from investigating pandemic fraud are being used to improve our investigatory efforts and passed on to the agencies tasked with administering benefit programs.

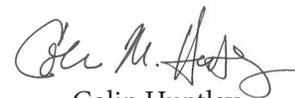
The Director of COVID-19 Fraud Enforcement and staff will continue to work closely with relevant Department of Justice components in the Criminal and Civil Divisions, our Strike Forces and U.S. Attorney's Offices, and our law enforcement partners to ensure that the government's response to COVID-19 fraud is effective, coordinated, and robust.



Michael C. Galdo
Director, COVID-19 Fraud Enforcement



Amanda L. Riedel
Deputy Director, Criminal
COVID-19 Fraud Enforcement



Colin Huntley
Deputy Director, Civil
COVID-19 Fraud Enforcement

CRIMINAL, CIVIL, and ASSET RECOVERY ACTIONS

II. Department of Justice

The Department of Justice continues to prioritize the investigation and prosecution of individuals and entities that committed pandemic program fraud. The Department has marshaled resources from U.S. Attorneys' Offices and the Criminal, Civil, Tax, and Antitrust Divisions to bring criminal, civil, and asset recovery actions against perpetrators of COVID-19 fraud. The Department supports a Director of COVID-19 Fraud Enforcement, two Deputy Directors of COVID-19 Fraud Enforcement, a lead prosecutor for the National Unemployment Insurance Task Force, a National COVID-19 Fraud Forfeiture Coordinator, a National COVID-19 Fraud Coordinator, and COVID-19 Fraud Coordinators in each U.S. Attorneys' Office. In 2023, the Department upscaled resources to address COVID-19 fraud by funding 50 term AUSA positions dedicated to COVID-19 fraud enforcement. And DOJ has stood up five COVID-19 Fraud Enforcement Strike Forces across six federal districts to pursue the most impactful criminal COVID fraud cases – those involving large amounts of loss, overseas actors, violent offenders, and perpetrators who defrauded multiple pandemic-era aid programs.

A. U.S. Attorneys' Offices

As of December 31, 2023, U.S. Attorneys' Offices criminally charged approximately 3,500 defendants in 2,388 pandemic fraud-related cases. Most of these cases involved unemployment insurance benefits fraud (UI), Paycheck Protection Program fraud

(PPP), and Economic Injury Disaster Loan fraud (EIDL), but other types of CARES Act fraud and health care fraud related to the COVID-19 pandemic were also charged. The fraud loss associated with these cases was more than \$2.1 billion.

U.S. Attorneys' Offices have criminally charged 3,500 defendants in pandemic fraud cases with associated losses of more than \$2B

As of December 31, 2023, approximately 2,005 defendants charged with pandemic-related fraud have pleaded guilty or been convicted at trial. The fraud loss associated with these completed cases is more than \$1.2 billion. While the number of resolutions is impressive, U.S. Attorneys' Offices have a similar number of investigations open that are yet to be charged.

Some examples of COVID-19 criminal fraud cases prosecuted by U.S. Attorneys' Offices include:

- In the Southern District of Georgia, a [Florida-based attorney was convicted at trial of conspiracy to fraudulently obtain almost \\$800,000 in Economic Injury Disaster Loans](#) for herself and others.
- In the Western District of Washington, [the ringleader of a \\$6.8 million pandemic fraud ring was sentenced to five years in prison](#) for fraudulently seeking funds from various relief programs.

- In the Eastern District of Washington, an Arkansas-based [business owner pleaded guilty to fraudulently receiving more than \\$16.5 million in SBA pandemic relief funds](#) for himself and others.

- In the Eastern District of Virginia, [a former VA nurse was sentenced to 18 years in prison for conspiring to fraudulently obtain more than \\$3.5 million](#) in UI benefits from at least five states. She and her co-conspirators filed more than 220 false applications for unemployment insurance benefits using stolen identities and the identities of state and federal prison inmates.

- In the Middle District of Florida, a [defendant was sentenced to eight years and six months in prison for obtaining more than \\$7.2 million in PPP loan funds](#), which he used to purchase Maserati and Mercedes-Benz cars and buy a 12-acre estate.

- The District of Minnesota has brought charges against more than 50 individuals for their respective roles in a [\\$250 million fraud scheme that exploited a federally funded child nutrition program](#) during the COVID-19 pandemic.

- In the Eastern District of Michigan, a man was sentenced to 15 years in prison for his role as the ringleader of conspiracies to use stolen identities to [fraudulently obtain \\$2.1 million in unemployment insurance benefits from multiple states and to traffic in methamphetamine](#).

In addition to, or as part of COVID-19 fraud criminal prosecutions, U.S. Attorneys’ Offices have pursued forfeitures and sought restitution orders in pandemic fraud matters. To date, COVID-19 fraud investigations in which the Department has been involved—including but not limited to investigations led by the Department of Justice, Department of Homeland Security, Department of Treasury, United States Postal Inspection Service, Department of Labor-Office of Inspector General, and Small Business Administration-Office of Inspector General—have resulted in significant civil and criminal forfeitures, restitution orders, and collaboration with private industry partners to combat fraud.

DOJ and law enforcement partners have obtained final forfeitures of over \$1B

For example, as of the end of 2023, forfeitures in civil administrative, civil judicial, and criminal judicial cases resulted in the final forfeiture of more than \$1 billion in fraud proceeds. Although criminal cases and forfeitures serve as a key tool in the prosecutorial mission to address COVID-19 fraud, in many instances, final forfeiture via civil administrative and civil judicial means facilitated the recovery of hundreds of millions of dollars when individual bad actors could not be located or extradited for criminal prosecution. Consistent with the Department’s goal of using forfeited assets to compensate victims, much of the finally forfeited money has been returned to victimized federal and state agencies and

financial institutions or is currently being processed for potential return to victims. Yet other money remains seized, pending additional process.

Enforcement efforts as of the end of 2023 in COVID-19 fraud-related criminal prosecutions for which statutes authorized restitution resulted in the issuance of over \$882 million in total restitution orders to both government and private victims.

Finally, outside of formal forfeiture seizure or restitution processes, federal law enforcement regularly consults with financial institutions that have received fraudulently obtained UI funds but now seek law enforcement input on the voluntary return of those funds to defrauded state workforce and unemployment agencies. Such informal efforts, wherein private actors seek law enforcement assistance in building bridges among appropriate financial institution, state agency, and DOL points of contact, have resulted in the return of billions of dollars in fraud proceeds outside of the forfeiture and restitution framework.

As of April 1, 2024, USAOs, in conjunction with the Civil Division, have also opened over 1,200 civil pandemic fraud matters, including more than 600 qui tam cases. Civil AUSAs and Civil Division attorneys obtained more than 400 judgments or settlements totaling over \$100M. These cases include PPP, EIDL, health care fraud, agricultural program fraud, and fraud on other pandemic-relief programs. Examples of these cases include:

- A Texas-based commercial roofing contractor and its nationwide network of roofing and disposal companies [agreed to pay \\$9 million](#) to resolve allegations that they violated the False Claims Act (FCA) by falsely certifying that eight of their affiliates were eligible to receive loans through the Small Business Administration's (SBA) Paycheck Protection Program (PPP).
- [A Georgia urgent care chain agreed to pay \\$1,600,000](#) to resolve allegations that they violated the False Claims Act (FCA) by submitting improperly upcoded Evaluation and Management claims to Medicare for the testing and treatment of patients with suspected exposure to COVID-19 during the Coronavirus pandemic.
- A California-based technology services company [agreed to resolve allegations that it knowingly violated the False Claims Act](#) when it applied for, received, and retained two Paycheck Protection Program (PPP) loans totaling \$400,000 in violation of PPP rules, falsely certifying that it met company size restrictions for the loans, and that its revenue decreased in excess of 25% from 2019 to 2020, a program requirement, when its revenue increased.

In addition, USAOs, through the Executive Office for U.S. Attorneys (EOUSA), have partnered with the Civil Division to develop and roll out database tools to detect and investigate fraud. This

includes the analysis of more than 225 million claims paid by the Health Resources and Services Administration's COVID-19 Uninsured Program and approximately 15 million PPP and EIDL loans. EOUSA has partnered with the Civil Division to provide training on using the databases to investigate fraud in these programs.

B. COVID-19 Fraud Enforcement Strike Forces

In September 2022, DOJ announced the establishment of [three COVID-19 fraud enforcement strike forces](#), which are housed in the U.S. Attorneys' Offices for the District of Maryland, Southern District of Florida, and a joint task force co-located in the Eastern and Central Districts of California. In August 2023, [two additional Strike Forces](#) were announced in the District of New Jersey and District of Colorado. The strike forces are comprised of dedicated prosecutors and agents from the Department of Labor Office of Inspector General, Small Business Administration Office of Inspector General, Department of Homeland Security Office of Inspector General, FBI, U.S. Secret Service, Homeland Security Investigations, Internal Revenue Service Criminal Investigations, and U.S. Postal Inspection Service, with assistance from the PRAC and the Special Inspector General for Pandemic Recovery. The OCDETF Fusion Center and OCDETF's International Organized Crime Intelligence and Operations Center, the Financial Crimes Enforcement Network, and the National Unemployment Insurance Fraud Task Force provide key support to the strike forces by providing leads, case intelligence, and deconfliction.

To date, strike force districts have charged more than 250 defendants with associated losses of over \$339 million

1. California Strike Force

The Eastern and Central Districts of California joint COVID Fraud Strike Force was formed in August 2022. As strike force district, the Eastern and Central Districts of California oversee agents, analysts, and AUSAs to bring the most impactful criminal pandemic fraud cases, often involving multiple CARES Act programs, foreign actors, violent perpetrators, or large loss amounts.

Since the inception of the Strike Force, the EDCA has criminally charged 17 cases with associated actual losses of over \$20 million, including:

- A defendant was sentenced to [81 months in federal prison for using stolen identities to claim over \\$9 million in fraudulent UI and EIDL benefits](#).
- A defendant, who was an inmate at the time of the offenses, was [sentenced to 84 months for participating in a conspiracy to use stolen identities to claim more than \\$1 million in UI payments](#), of which the conspirators fraudulently obtained over \$890,000.
- A former gang member and inmate at the time of the offenses was [sentenced to 65 months in prison for his role in \\$25 million UI fraud scheme](#).

EDCA prosecuted a gang member for fraudulently claiming \$25M in UI benefits

- A [woman was sentenced to 75 months in prison](#) for using stolen identities to claim over \$350,000 in UI and SBA benefits, of which she successfully obtained approximately \$200,000.

The EDCA has also successfully forfeited funds derived from pandemic fraud. In one case, the government secured an order of [forfeiture for the lead defendant's new condominium in Nigeria](#), which was purchased with UI fraud proceeds.

The EDCA continues to investigate and prosecute all manner of pandemic fraud. For example, in February 2024, the [EDCA charged several defendants in a case involving the CARES Act Employee Retention Credit](#). The charged conduct, orchestrated from prison, involved defendants conspiring to pursue over half a billion dollars in federal tax credits that were meant to help struggling businesses during the COVID-19 pandemic.

The Central District of California has joined with FBI, IRS CI, SBA-OIG, HHS-OIG, DOL-OIG, TIGTA, USSS, and several local law enforcement agencies to initiate 37 criminal cases involving 72 individuals suspected of committing PPP, EIDL, UI, and ERC fraud, with losses identified of more than approximately \$126 million. Approximately 15 of the 35 cases involve fraudulent UI claims with collective losses of more than \$53 million. CDCA's cases have covered a broad spectrum of criminal activity in its diverse population with a view

toward achieving just results and significantly deterring fraud involving taxpayer-funded programs.

In one CDCA prosecution, a jury convicted a ring of defendants who fraudulently obtaining more than \$20 million in PPP and EDIL funds. The lead defendant fled the U.S. and was sentenced *in absentia* to [17 years in prison](#). In another matter, a defendant pleaded guilty and was [sentenced to 30 months' imprisonment](#) for fraudulently obtaining more than \$500,000 in UI benefits using names of dozens of California state prison inmates.

CDCA convicted at trial a ring of fraudsters who fraudulently obtained \$20M in SBA loans

In April 2023, CDCA participated in a nationwide sweep to combat COVID stimulus-related and health care fraud. In one case, a physician and two other individuals were [charged](#) with submitting over 70 fraudulent PPP and EIDL applications and fraudulently obtained over \$3 million. The physician was also charged with allegedly submitting more than \$200 million in false claims to the Health Resources and Services Administration (HRSA) COVID-19 Uninsured Program, a program designed to prevent the further spread of the pandemic by providing access to uninsured patients for testing and treatment.

CDCA and its law enforcement partners have seized and forfeited over \$450,000 in UI-related cases and nearly \$2 million in SBA loan fraud cases.

CDCA has continued to increase its staffing to combat pandemic program-related fraud. COVID fraud cases are worked by criminal AUSAs across the district, in the Major Frauds, Violent and Organized Crime, and General Crimes Sections. CDCA has also hired an attorney from IRS CT Counsel's Office to fill a dedicated Covid Strike Force SAUSA position to focus on tax-related pandemic fraud matters.

2. District of Maryland Strike Force

Since the creation of Maryland's COVID-19 Strike Force, the U.S. Attorney's Office for the District of Maryland (USAO-MD) has handled more than 80 criminal investigations into COVID-19 fraud, with overall potential losses totaling more than \$100 million. At least 30 defendants have been criminally charged with COVID-19 fraud-related offenses involving alleged loss amounts exceeding \$55 million. USAO-MD currently dozens of open COVID-19 fraud investigations and prosecutions with cumulative losses exceeding \$70 million. In support of these efforts, the Maryland Strike Force currently has five dedicated criminal AUSAs and a paralegal working on pandemic fraud matters as well as criminal AUSAs outside of the strike force handling significant COVID-related cases. The district also has numerous active civil fraud cases pending with tens of millions of dollars in associated potential losses.

In June 2021, the State of Maryland flagged an astonishing 1.3 million UI claims as potentially fraudulent. Accordingly, UI fraud makes up a large portion of USAO-MD Strike Force investigations. Some notable UI

fraud cases from the Maryland Strike Force include:

- [The U.S. Attorney's Office charged six individuals, including two Maryland State Department of Labor subcontractors, with participating in a conspiracy to fraudulently obtain approximately \\$3.5 million in UI benefits.](#) The lead defendant faces separate narcotics and firearms charges, including allegations that he unlawfully possessed a machine gun in furtherance of a drug trafficking crime.
- Eleven individuals were [charged in connection with a \\$1.6M UI fraud conspiracy](#) involving aggravated identity theft. Five of the nine defendants have pleaded guilty and two of the defendants have each been [sentenced to more than four years in prison.](#)

The USAO-MD currently has more than 30 SBA loan fraud investigations and prosecutions, with anticipated losses exceeding \$40 million. For example, a [defendant pleaded guilty](#) in October 2023, to submitting more than \$17.9 million in fraudulent CARES Act loan applications on behalf of himself and his coconspirators, using the illicitly obtained funds to travel internationally, purchase property in Egypt, and open a beachfront restaurant.

The USAO-MD has targeted cases with connections between COVID-19 fraud and individuals involved in violent crime, organized criminal networks, business email compromise schemes, and narcotics distribution. Using probable cause from the commission of COVID-19 fraud, agents

have conducted searches and seized illegal firearms, narcotics, and stolen personally identifying information. The USAO-MD Strike Force continues to investigate and charge violent and drug offenders who committed pandemic program fraud as part of the U.S. Attorney’s “Al Capone” strategy to get guns and violent criminals off Maryland’s streets. For example:

- A convicted felon was charged with [CARES Act fraud](#) as well as firearm offenses and possession with the intent to distribute fentanyl.

D-Maryland defendant sentenced to 7 years in prison for COVID-19 fraud found with an illegal machine gun

- A defendant was [sentenced to seven years](#) in federal prison for committing PPP, EIDL, and UI fraud, with actual losses of more than \$1 million and attempted losses of \$3 million. When the government executed search warrants in the case, agents recovered stolen identifying information and ghost guns, including one modified to function as a machine gun.
- A defendant [pleaded guilty](#) to submitting more than \$3.5 million in fraudulent COVID-19 PPP and EIDL applications and using fraudulently obtained funds to pay for a vacation, a Mercedes-Benz, jewelry, and luxury goods, including items from Luis Vuitton, Neiman Marcus, Dior, Cartier, Gucci, Chanel, and Hermes. During a search of a residence at the time of arrest,

law enforcement agents recovered four firearms.

3. Southern District of Florida Strike Force

Since the creation of the Southern District of Florida’s COVID-19 Strike Force, the U.S. Attorney’s Office for the Southern District of Florida (SDFL) has charged more than 50 defendants with COVID fraud-related offenses involving alleged loss amounts exceeding \$76 million. In support of these efforts, SDFL currently has four dedicated criminal AUSAs working on criminal pandemic fraud cases and investigations, as well as criminal AUSAs outside of the strike force handling significant COVID-related matters.

Examples of SDFL’s Strike Force efforts include:

- The SDFL indicted 17 [employees of the Broward Sheriff’s Office were charged](#) with obtaining fraudulent PPP/EIDL loans. One former deputy was recently [convicted at trial](#), several employees have pleaded guilty, and other defendants’ cases are still pending.

17 Broward County Sheriff’s Office employees charged with PPP fraud

- [A defendant was sentenced](#) to 71 months in prison for fraudulently obtaining PPP and EIDL loans and Shuttered Venue Operator Grants (SVOG), using the stolen funds to buy two Tesla S models, a Lamborghini, a Porsche, a diamond Audemars Piguet

watch, a rose gold and diamond pendant with his company's logo, a half-kilogram gold chain with 70 carats of diamonds, and a 1-kilogram gold chain.

- A former contract detention officer at the federal Krome Detention facility who was the [leader of a PPP fraud ring](#) was sentenced to 32 months in prison for preparing fraudulent PPP applications in return for kickbacks.
- A defendant was [sentenced to 70 months](#) in prison for laundering the over \$2 million in fraudulently obtained PPP and EIDL loans and using the funds to gamble and to pay for cosmetic surgery, a Cadillac Escalade, and a Pomeranian puppy.
- A defendant was [sentenced to 41 months](#)¹ in prison and ordered to pay \$643,000 in restitution for his role in a conspiracy to use stolen identities to fraudulently obtain more than \$1.1 million in UI funds. His coconspirators were each sentenced to 33 months in prison.

4. District of New Jersey Strike Force

In August 2023, the District of New Jersey launched its COVID-19 Fraud Strike Force, which built upon the previously established COVID-19 Fraud Task Force. Since the start of the pandemic, the District of New Jersey has charged approximately 104 defendants with COVID-19 fraud.

At present, the District of New Jersey has four criminal AUSAs dedicated to prosecuting COVID-19 fraud cases on a full-time basis. On January 25 and 26, 2024, the District of New Jersey hosted a two-day strike force coordination meeting, which had over 60 participants. Currently, 12 partner agencies participate in the New Jersey Strike Force, with 25 dedicated agents and investigators supporting the strike force's efforts.

Since the inception of the COVID-19 Fraud Strike Force in August 2023, the District of New Jersey has charged approximately 18 individuals with COVID-19 loan fraud and fraud committed in connection with obtaining unemployment benefits and tax stimulus payments. Approximately seven COVID-19 fraud defendants have been sentenced, resulting in restitution orders totaling more than \$5 million. For example, co-defendants indicted in a [\\$3.75 million PPP fraud scheme](#) are set to be tried in July 2024.

The District of New Jersey currently has approximately 25 unresolved charged COVID-19 fraud cases and is overseeing dozens of ongoing pandemic fraud investigations. The District of New Jersey remains committed to prosecuting fraudsters in New Jersey and throughout the country who stole much-needed funds from small business and families during the pandemic.

5. District of Colorado Strike Force

In August 2023, the District of Colorado launched its COVID-19 Fraud Strike Force. Since the start of the pandemic, the District of Colorado and partner agencies participating in the strike force have devoted significant

¹ See p. 6.

resources to combatting COVID-19 fraud committed in Colorado and around the country. The District of Colorado has four criminal AUSAs working on its COVID-19 Fraud Strike Force, including two term AUSAs hired in the first quarter of 2024. Additionally, the District of Colorado has ten civil AUSAs, along with support staff, working on False Claims Act investigations involving COVID-19 fraud.

To date, the District of Colorado has charged more than 20 individuals with COVID-19 loan fraud and fraud committed in connection with obtaining UI benefits and tax stimulus payments. Of those, 12 defendants have been convicted and sentenced, resulting in restitution orders totaling more than \$14 million. Two additional defendants have pleaded guilty and are awaiting sentencing.

For example, the District of Colorado [charged four defendants](#) with a wire fraud and money laundering conspiracy. The indictment alleges that the conspirators fraudulently obtained more than \$8 million in COVID-19 business loans, unemployment benefits, tax refunds, and tax stimulus payments using the names of identity-theft victims. In another case, a defendant was [sentenced to 51 months' imprisonment](#) and ordered him to pay more than \$1 million in restitution for preparing and submitting fraudulent PPP loan applications.

D-Colorado and law enforcement partners seized over \$1B in fraudulently obtained EIDL funds

The District of Colorado has also worked closely with law enforcement partners to seize more than \$1 billion in wrongfully obtained EIDL assets, as well as to forfeit houses, vehicles, cryptocurrency, and bank accounts. The District of Colorado obtained a seizure warrant that led to the seizure of over 15,000 accounts and approximately \$286 million in fraudulently obtained EIDLs, which funds the U.S. Secret Service ultimately returned to the SBA.

C. Criminal Division

1. Fraud Section

The Fraud Section has continued to expand its efforts to combat COVID-19-related fraud both in the Market Integrity and Major Fraud (MIMF) Unit and the Health Care Fraud Unit (HCF). The Fraud Section maintains its focus on programs created or expanded by the CARES Act, including PPP and EIDL programs, Provider Relief Fund (PRF) programs, and Health Resources and Services Administration's COVID-19 Uninsured Program (UIP). The HCF Unit has targeted individuals and entities that are took advantage of COVID-19 testing programs, including CMS's COVID-19 over-the-counter test kit demonstration. Since August 2022, the HCF Unit, in partnership with various U.S. Attorney's Offices and law enforcement agencies, has charged 19 defendants for COVID-19-related fraud involving more than \$393 million in alleged loss, while the MIMF Unit has charged 63 defendants involving more than \$116 million in intended loss. The MIMF Unit has continued its enforcement efforts through 11 trials of COVID fraud cases in the last two

years. For example, the MIMF Unit and its U.S. Attorney’s Office partners prosecuted a total of 16 defendants, all of whom were convicted in the Southern District of Texas for engaging in a conspiracy to fraudulently obtain more than \$20 million in PPP loans. The [ringleader of the conspiracy was sentenced to 15 years in prison](#).

Since 2022, the Fraud Section and USAO partners have criminally prosecuted 82 defendants for COVID-19 fraud with associated losses over \$500M

In April 2023, the HCF Unit, along with its U.S. Attorney’s Office and law enforcement partners, announced its largest Nationwide Coordinated Law Enforcement Action to Combat COVID-19 Health Care Fraud. Building on the success of prior years’ COVID-19 enforcement actions, the HCF Unit announced criminal charges against 18 defendants across nine federal districts for alleged participation in various fraud schemes involving health care services that exploited the COVID-19 pandemic and allegedly resulted in over \$490 million in COVID-19-related false billings to federal programs and theft from federally funded pandemic programs. The enforcement action included seizures of more than \$16 million. These charged schemes include: (a) the submission of fraudulent claims to the UIP for services not provided and services that were not medically necessary, (b) the buying and selling of Medicare beneficiary identification numbers that were used to bill Medicare for COVID-19 over-the-counter test kits, (c) the manufacture and distribution of fake

COVID-19 vaccination cards, and (d) the submission of fraudulent loan agreements, attestations, and other documentation to obtain millions in PRF and EIDL funds. In one such case from the Central District of California, the Fraud Section’s HCF Unit secured [a ten-year prison sentence](#) for a man who operated a laboratory that fraudulently billed Medicare for \$234 million in lab tests, including COVID-19 testing. The defendant was also ordered to forfeit over \$31 million and ordered to pay more than \$31 million in restitution.

2. Money Laundering and Asset Recovery Section

The Money Laundering and Asset Recovery Section (MLARS) continues to work in coordination with the CFETF, EOUSA, the Justice and Treasury asset forfeiture funds, and law enforcement agencies, on forfeiture of the proceeds of CARES Act-related fraud and the return of forfeited funds to victim agencies and financial institutions. MLARS’ Program Management and Training Unit (PMTU) will continue working with SBA, Labor, and other agencies and financial institutions to return forfeited funds through the restoration and remission programs overseen by PMTU.

3. Office of International Affairs

Since the start of the pandemic, the Office of International Affairs (OIA) has partnered with domestic prosecutors and agents, and with foreign authorities, to combat transnational crimes flowing from the pandemic. OIA is instrumental in securing mutual legal assistance (MLA) and

extradition in connection with investigations and prosecutions. Examples of OIA assistance include over 80 incoming MLA requests from around the world seeking evidence for use in foreign investigations and prosecutions related to the pandemic. OIA has opened dozens of MLA matters related to pandemic-based fraud to countries in Africa, Asia, Europe, and North America. In February 2023, OIA assisted in the [extradition](#) of a defendant from Germany to the Western District of Washington, where he is charged with a multimillion-dollar scheme to defraud U.S. government programs of at least US \$2.4 million, the majority of which constituted COVID-19 UI benefits. In April 2023, OIA assisted with the removal of a defendant from Thailand via deportation to face PPP-related fraud charges in the Central District of California. Additionally, OIA has made several outgoing extradition requests seeking multiple individuals wanted for large-scale pandemic relief fraud.

D. Civil Division

1. Civil Fraud Section

The Commercial Litigation Branch, Fraud Section, has primary responsibility for enforcing the False Claims Act (FCA), the government’s primary civil tool to redress fraud impacting federal funds, and the Financial Institutions Reform Recovery and Enforcement Act of 1989 (FIRREA), which provides for civil penalties for certain financial crimes. Since the start of the COVID-19 pandemic, CIV-Fraud has partnered closely with U.S. Attorneys’ Offices nationwide on an unprecedented surge in civil fraud investigations relating

to pandemic relief programs. In addition to combatting fraud in connection with SBA programs, CIV-Fraud continues to lead investigations into virtually every aspect of the government’s pandemic relief efforts, including state and local governments and tribal entities that received grants; government procurements for PPE and other essential goods; and payment advances and grants to health care providers during the pandemic. It also is investigating a wide range of health care fraud matters, including those alleging misconduct in connection with COVID-19 testing and treatment.

The CIV-Fraud Section spearheaded the creation, implementation, and expansion of its customized data platforms to analyze and detect fraud across approximately 15 million PPP and EIDL loans and more than 225 million claims paid by the Health Resources and Services Administration’s COVID-19 Uninsured Program. These tools have been used by scores of attorneys, auditors, and investigators across nearly all U.S. Attorneys’ Offices, as well as the FBI and DOJ Asset Forfeiture teams, to generate high-value investigative leads and to examine and prioritize voluminous referrals. In addition, the CIV-Fraud Section has continued to provide training to U.S. Attorneys’ Offices, Offices of Inspectors General, and external stakeholders on a wide range of pandemic relief programs and civil enforcement tools.

CIV-Fraud and USAOs have obtained more than 400 False Claims Act settlements and judgments totaling over \$100M

To date, CIV-Fraud has opened more than 1,200 new investigations relating to potential fraud in connection with multiple pandemic relief programs. These include investigations implicating more than 6,000 individuals and entities and billions of dollars in pandemic relief funds. As of April 1, 2024, USAOs, in conjunction with the Civil Division, have also opened over 1,200 civil pandemic fraud matters, including more than 600 *qui tam* cases. Civil AUSAs and Civil Division attorneys obtained more than 400 judgments and settlements totaling over \$100M. Notable examples include:

- A Florida-based automotive management company [agreed to pay more than \\$9 million](#) to resolve allegations that it knowingly violated the FCA by providing false information relating to its corporate affiliations and size in support of a PPP loan forgiveness application.
- A New Jersey public relations firm [paid \\$2.24 million](#) to resolve allegations that it knowingly violated the FCA by falsely certifying its compliance with PPP requirements even though it was ineligible for the loan due to its status as a registrant under the Foreign Agent Registration Act.
- A Georgia-based clinical laboratory, along with its owner, [agreed to pay more than \\$13 million](#) to resolve allegations that it sought to profit off the COVID-19 pandemic by paying independent contractor sales representatives to recommend expensive and medically unnecessary respiratory pathogen panels to senior communities that were interested only in COVID-19 tests.

The Department has seen a steady increase in the number of new *qui tam* actions filed under the False Claims Act alleging fraud in connection with pandemic relief programs, with year-over-year increases from 2020 through 2023. Combined with the growing number of investigative leads developed through data analytics, the Civil Fraud Section anticipates that civil pandemic fraud enforcement will continue to require substantial resources for years to come.

2. Consumer Protection Branch

The Consumer Protection Branch has pursued actions against distributors of fake COVID-19 treatments and cures, as well as other individuals and entities engaged in conduct that threatens the health of consumers. Throughout the pandemic, the Branch brought civil and criminal cases, including actions against sellers of fraudulent COVID treatments, purveyors of faulty PPE, individuals who deliberately tampered with COVID vaccines, and those selling fraudulent covid products online. Some of these actions were brought under the new COVID-19 Consumer Protection Act, which was signed into law in December 2020. For example, in August 2023 the Branch secured a [\\$1 million judgment](#) against a company and individual that marketed vitamin supplements as providing equal or better protection against COVID-19 than vaccines. The Branch also pursued ongoing litigation during 2023 against entities that allegedly sold products such as tea or nasal spray as COVID-19 cures or treatments. Additionally, the Branch, along with USFIS and FBI, continues to lead an [annual campaign to disrupt money mule networks](#)—including those used to move stolen pandemic-relief funds.

E. Tax Division

The Tax Division has focused its efforts regarding COVID-19 fraud on combating abuse of the Employee Retention Credit (“ERC”). A substantial part of this effort involves providing training and guidance about the topic to prosecutors throughout the country. For example, the Division presented a nationwide training through the Executive Office of United States Attorneys on how to investigate and charge ERC fraud. The Tax Division also published an [article](#) in the DOJ’s Journal of Federal Law and Practice, providing an overview of COVID-related tax fraud, including the ERC. Tax Division attorneys have provided trainings on ERC-related crimes to criminal and civil enforcement personnel at the IRS.

Tax Division and D-NJ charged a tax preparer with filing thousands of tax returns claiming fraudulent COVID tax credits

Tax Division trial attorneys are directly involved in the prosecution of ERC fraud. The Division has assigned a trial attorney to each of the COVID-19 fraud strike forces to develop investigations into ERC schemes. Tax Division prosecutors have also added ERC cases to their regular litigation dockets. In one notable example, along with the U.S. Attorney’s Office for the District of New Jersey, the Tax Division [charged a defendant](#) with preparing more than a thousand false tax returns seeking tens of millions of dollars in refunds based on the ERC and the COVID-related Sick and Family Leave Credit.

Because the ERC was available for relatively recent years (2020 and 2021) and given the complexity of identifying and prosecuting these offenses, the Tax Division expects that prosecuting ERC-related crimes will continue to be a priority for the foreseeable future.

F. Antitrust Division

Since the start of the COVID-19 pandemic, the Department of Justice’s Antitrust Division has fulfilled its mission—the promotion of economic competition through enforcement of antitrust laws and principles. The Antitrust Division adopted a multi-faceted COVID-19 response, particularly as it pertains to fraud and related crimes impacting competition. The Antitrust Division’s initial response to the pandemic, which included widespread public messaging about the intersection of competition law and the whole-of-government response to the public health emergency, has matured into more targeted outreach and enforcement.

The Antitrust Division’s response to the COVID-19 pandemic also includes its continued leadership of the Department’s Procurement Collusion Strike Force (“PCSF”) and an active program of outreach, engagement, and training. The PCSF, which is the Department’s coordinated, national, inter-agency answer to collusion and other schemes targeting government spending at all levels, continued its efforts in the face of crisis-related disruptions. Since August 2022, the PCSF has trained other law enforcement agency partners, frontline agencies responsible for disbursing and overseeing federal grants, state officials from

offices of attorneys general and procurement agencies, and private-sector groups in the healthcare, compliance, education, and other sectors.

In an Antitrust case, seven companies agreed to pay over \$681M in criminal penalties for illegally raising the price COVID-19 drugs

In 2022-2023, the PCSF collaborated with the PRAC to develop a series of data analytic dashboards that identify federal government contractors believed to be at a higher risk for misusing pandemic relief funding. The dashboards identified contractors who met one of multiple sets of criteria. One set of criteria was developed using data obtained by the Executive Office for the United States Attorneys, and the others were developed using publicly- and non-publicly available spending and identification data. Pursuant to an agreement between the PRAC and the Antitrust Division, the PCSF shared these

dashboards with approximately twenty data and law enforcement personnel from nearly a dozen oversight agencies to aid in their proactive data analytics efforts. In 2024, the PCSF will distribute judicial district-specific dashboard results to PCSF representatives throughout the country to focus joint law enforcement efforts on local high-risk contractors. In August 2023, the Antitrust Division announced the final resolutions in investigation into criminal conduct by generic pharmaceutical companies. The Antitrust Division, the U.S. Attorney's Office for the Eastern District of Pennsylvania, the FBI, and the U.S. Postal Service Office of Inspector General uncovered price-fixing, bid-rigging and market-allocation schemes affecting many generic medicines, including illegally raising the prices of prescription drugs necessary to treat or reduce the risk of conditions known to amplify or worsen the effects of a COVID-19 infection. All told, the seven generic drug company defendants collectively agreed to pay more than [\\$681 million in criminal penalties](#).

TASK FORCES

III. National Unemployment Insurance Fraud Task Force

In late 2020, in response to massive pandemic UI fraud, the Office of the Deputy Attorney General created the National Unemployment Insurance Fraud Task Force (NUIFTF). Although originally focused on UI fraud, the task force has expanded to collect and analyze data related to all manner of CARES Act fraud. The NUIFTF is headed by a lead prosecutor and is comprised of agents, analysts, and data scientists from DOL-OIG, FBI, HSI, USSS, IRS-CI, SBA-OIG, USPIS, SSA-OIG, DHS-OIG, and the PRAC. Among other things, the task force works closely with DOJ's Organized Crime Drug Enforcement Task Forces' (OCDETF) International Organized Crime Intelligence and Operations Center (IOC-2) and DOL-OIG to identify the largest perpetrators of COVID-19 fraud, focusing on transnational criminal networks. The NUIFTF and IOC-2 oversee the collection and sharing of data related to unemployment insurance claims and SBA loan information for an intergovernmental approach to identifying patterns of fraud and sharing best practices for data science and intelligence.

The NUIFTF, a first-of-its-kind task force generating actionable leads against foreign actors and crime syndicates committing cyber-enabled fraud, has disseminated over 100 leads and intelligence associated with over \$3B in suspected pandemic fraud

The NUIFTF acts as a first-of-its-kind lead generator for agents and prosecutors. The task force focuses on criminal networks and using data analytics to identify foreign actors who committed not just pandemic-era fraud, but routinely perpetrate romance scams, BEC scams, and other types of cyber-enabled fraud. To date, the NUIFTF initiated approximately 189 pandemic fraud leads and has transmitted more than 100 leads to agencies and USAOs, each with dozens, if not hundreds, of associated fraudulent UI, PPP, and EIDL claims. The NUIFTF also developed intelligence to enhance ongoing investigations to assist in the identification of criminal conduct and actors. To date, the intelligence generated by the NUIFTF represents over \$3.3B in suspected pandemic fraud.

For example, the NUIFTF sent a lead to the Western District of Washington involving approximately \$25 million in attempted COVID fraud, consisting of over 1,700 fraudulent claims for UI benefits filed in over 25 states, all of which involved the use of stolen identities. The lead led to the indictment of two defendants, one of which, a Nigerian national, was [sentenced to 42 months' imprisonment](#) after being extradited from Germany. The second defendant, also a Nigerian national, is awaiting [extradition from Canada](#).

The NUIFTF has several key functions, all of which are ongoing and remain crucial in the continued pursuit of COVID-19 fraud enforcement:

- The NUIFTF assisted in the creation of the five Covid Fraud Strike Forces and provides high value leads to each Strike Force, many of which involve foreign targets.
- The NUIFTF provides investigators with a central location where searches of multiple pandemic relief data sets can be conducted, rather than having to pursue data that was previously siloed within various state and federal agencies.
- The NUIFTF has provided COVID fraud investigation trainings to federal law enforcement, local law enforcement, and USAOs across the country.
- The NUIFTF joined with the FBI's Safe Streets Task Force and DOL-OIG to initiate and pursue a violent offender pandemic fraud program in multiple cities across the United States. That ongoing initiative seeks to identify violent offenders under criminal investigation who also participated in pandemic program fraud.

The NUIFTF continues to regularly receive millions of new data points from state workforce agencies and other sources that will enable the refinement of existing leads and the creation of new COVID-19 fraud leads for the foreseeable future.

IV. Pandemic Response Accountability Committee

The 2020 CARES Act created the Pandemic Response Accountability Committee (PRAC) to promote transparency

and support oversight of the federal government's COVID-19 pandemic response. The PRAC coordinates with 20 member Offices of Inspectors General (OIG) to oversee more than \$5 trillion in COVID-19 spending, identify major risks that cross program and agency boundaries, and detect fraud, waste, abuse, and mismanagement of relief funds. The PRAC also provides timely, accessible, and comprehensive spending data on its website, [Pandemic Oversight - Home | Pandemic Oversight](#).

The PRAC's efforts have led to 127 investigations, over 60 defendants charged, 44 years in collective prison time, and \$11M in restitution

The PRAC Fraud Task Force is a key component of the organization's cross-cutting efforts. Comprised of more than 50 agents from over a dozen member OIGs, the PRAC Fraud Task Force investigates cases in pandemic programs with significant fraud, such as SBA's EIDL and PPP loans. As of January 2024, the PRAC Fraud Task Force's efforts have resulted in 127 investigations with over 60 individuals charged, 44 years in collective prison time, and \$11 million in court-ordered restitution. In the PRAC Fraud Task Force's largest investigation to date, 14 individuals were charged in an alleged [\\$53 million PPP fraud scheme](#). Allegedly, several of these individuals used a group of affiliated recycling companies to submit at least 29 fraudulent PPP loan applications that included inflated payroll expenses, doctored bank statements, and false tax forms to financial institutions.

In addition to conducting investigations through the collective power of its OIG partners, the PRAC also provides robust investigative support to law enforcement partners in a variety of ways. The Pandemic Analytics Center of Excellence (PACE) offers data management, advanced analytic capabilities, and investigative lead generation for the PRAC Fraud Task Force, DOJ COVID-19 Fraud Enforcement Task Force, and other OIG and law enforcement organizations. As of January 2024, the PACE has provided investigative support to more than 45 federal law enforcement and OIG partners in over 700 pandemic-related investigations—all in less than four years since the PRAC’s inception. With over 8,000 subjects and an estimated fraud loss of \$1.87 billion associated with these investigations, the PACE has demonstrated a valuable return on investment.

The PACE serves as a force multiplier for the PRAC’s OIG and law enforcement partners due to its ability to share data, resolve entities (i.e., recipients) across data sources, and detect potentially suspicious networks across agencies and programs. The PACE has access to 47 government, public, and non-public data sets, and has established Memorandums of Understanding with 47 OIGs and law enforcement agencies to prevent and detect improper payments and fraud across federal benefits programs. Additionally, the PRAC has recruited, hired, and placed 28 employees across the OIG community through its Data Science Fellows Program, providing partners with specialized talent to help them conduct data analytics within their pandemic programs.

In January 2023, the PRAC issued a Fraud [Alert](#) in which the PACE and its team of data scientists identified more than 69,000 questionable Social Security Numbers that were used to obtain \$5.4 billion in potentially fraudulent pandemic loans.

In February 2023, PRAC Chair Michael E. Horowitz [testified](#) along with other federal oversight leaders before the House Committee on Oversight and Accountability and the House Committee on Ways and Means and shared the benefits of using advanced data analytics to identify fraud in pandemic relief programs. In November 2024, Chair Horowitz [testified](#) to the Senate Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs. The Chair encouraged Congress to make the PACE permanent as a tool to help watchdogs oversee all federal spending, including future emergency relief and recovery programs.

Beyond partnerships with federal agencies, the PRAC supports and coordinates with state and local law enforcement. The PRAC continues to hold quarterly briefings with state and local officials, including law enforcement and auditing professionals, to share valuable insights on fraud indicators, patterns, and evolving schemes. Additionally, the PRAC focuses on empowering individuals and whistleblowers to report alleged wrongdoing using the hotline on PandemicOversight.gov. To date, the PRAC has received over 9,000 hotline complaints that have been routed to relevant agencies for further action as appropriate.

INVESTIGATIVE AGENCIES

V. Department of Labor, Office of Inspector General

The U.S. Department of Labor, Office of Inspector General (DOL-OIG) focused on leveraging government partnerships and private-sector relationships to: (i) bring early pandemic UI fraud investigations to successful resolutions; (ii) complete high impact audits concerning systemic issues facing DOL and state workforce agencies (SWAs) regarding pandemic UI programs, and (iii) appropriately support the NUIFTF's and COVID-19 Fraud Enforcement Task Force's (CFETF) efforts to identify significant pandemic fraud leads focused on complex criminal schemes; cases involving substantial loss; street-level enterprises; and transnational/international actors. To that end, DOL-OIG:

- Provided training to thousands of internal and external stakeholders, such as state auditors/comptrollers/treasurers, chief financial officers, state and federal UI program representatives, the National Association of State Workforce Agencies, the International Criminal Police Organization, multi national law enforcement investigative teams, and foreign law enforcement partners;
- Released multiple alerts and other products to DOL, SWAs, and private-sector partners; and
- Continued to bolster multi-directional intelligence sharing and investigative leadership by dedicating additional

resources to the International Organized Crime Intelligence and Operations Center, and engaging with public/private alliances, such as the National Cyber-Forensics and Training Alliance.

DOL-OIG's oversight of the UI program has resulted in 1,128 criminal convictions with defendants sentenced to a collective 24,850 months in prison

Since the beginning of the pandemic, DOL-OIG's investigative efforts in this space have continued to be unprecedented and include opening over 205,000 matters related to UI fraud, with approximately 14,500 matters opened since August 2022. Since April 1, 2020, the pandemic UI investigative work by DOL-OIG has yielded impressive results with the agency obtaining a total of 1,702 indictments/initial charges, executing over 850 search warrants, obtaining 1,128 convictions with over 24,850 months of incarceration ordered, and more than \$1 billion in monetary recoveries. Even amidst budget constraints, DOL-OIG continues to expend significant resources addressing considerable post pandemic UI fraud issues with DOL and SWAs. Between August 2022 and December 31, 2023, this has resulted in 512 individuals being charged and another 531 defendants convicted of crimes related to UI fraud. Between August 2022 and December 31, 2023, DOL-OIG's UI investigations have resulted in more than \$145 million in investigative monetary results. DOL-OIG's Offices of Investigation

and Audit have conducted analyses and audits of the UI program. During this time, they have identified: state disbursements of \$9.9 billion in pandemic UI benefits to individuals likely committing fraud; \$30.9 billion in suspicious UI payouts in six high-risk categories; and continued activity by organized criminal groups that are exploiting UI programs by adapting their methods to bypass safeguards and target system vulnerabilities. Additionally, DOL-OIG's criminal investigators, data scientists, and analysts have substantially assisted in the generation and referral of approximately 30 high-impact pandemic fraud leads to NUIFTF partner agencies across the United States.

Finally, the DOL Inspector General provided congressional testimony on multiple occasions, outlining the scope and magnitude of the historic levels of fraud, waste, and abuse in pandemic UI programs.

More information related to DOL-OIG's pandemic work can be found on DOL-OIG's Pandemic Response [website](#).

VI. Small Business Administration, Office of Inspector General

Since 2020, SBA-OIG's oversight of the PPP and EIDL programs has resulted in approximately 1,255 criminal indictments, 985 arrests, and 683 convictions as of December 31, 2023. SBA-OIG has identified over \$1B in forfeitable COVID fraud proceeds and more than \$10B in disallowed costs through audits and reviews. Some examples of SBA-OIG investigated fraud include:

SBA-OIG's oversight of the PPP and EIDL programs has resulted in 1,255 indictments and 683 convictions

- A former reality television star was [sentenced](#) to more than 17 years in prison related to a Ponzi scheme and charges involving fraudulent PPP loan applications.
- A Texas man was [sentenced to nine years in prison](#) for using fraudulently obtained PPP loans to purchase a Lamborghini, Rolex, and other luxury goods.
- Members of a [California fraud ring](#) were convicted for using fake or stolen identities to submit approximately 150 fraudulent federal pandemic relief loans for sham businesses, for which they received more than \$20 million.

Since March 2020, SBA-OIG has initiated over 1,000 investigations involving complaints of fraud; received more than 270,000 SBA-OIG Hotline complaints; and, using data analytics, identified more than 104,000 actionable leads. Given the extension of the statute of limitations for SBA loan fraud related to the pandemic, SBA-OIG and its law enforcement partners anticipate that the criminal and civil prosecution of these leads will continue for the foreseeable future.

In addition to criminal and civil cases, SBA-OIG has worked to return more than \$28 billion in EIDL funds from financial institutions and borrowers. And, because of

our oversight work published in OIG Reports, [Report 23-16: Ending Active Collections on Delinquent COVID-19 Economic Injury Disaster Loans](#) and [Report 22-15 SBA’s Guaranty Purchases for Paycheck Protection Program Loans](#), the agency has completed a comprehensive cost benefit analyses to substantiate the pursuit of collections on \$30 billion in EIDL and PPP loans under \$100,000.

In June 2023, SBA-OIG published the [COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape](#) report due the unprecedented levels of fraud in these pandemic relief programs. The report estimates that SBA disbursed over \$200 billion in potentially fraudulent COVID-19 EIDLs, EIDL Targeted Advances, Supplemental Targeted Advances, and PPP loans.

SBA-OIG, together with its law enforcement partners, continues to prioritize the integrity, efficiency, and effectiveness of SBA programs. SBA-OIG’s response to pandemic fraud to date demonstrates that SBA-OIG, together with its law enforcement partners, provides independent, objective, and timely oversight of SBA while seeking to return funds to the taxpayers where appropriate and punish wrongdoers.

VII. Federal Bureau of Investigation

The Federal Bureau of Investigation continues to work in coordination with the DOJ and federal, state, and local law enforcement and regulatory partners, as well as partners in the private sector, to detect and disrupt COVID-19-related fraud. This work spans multiple FBI Divisions and programs.

The FBI has initiated 364 COVID-19-related health care fraud investigations into medical providers, laboratories, and others engaging in health care fraud schemes, including but not limited to overbilling or “upcoding” for services, billing for services not rendered, performing and billing for medically unnecessary services, telemedicine/telehealth, fraud, kickback schemes, and identify theft. The FBI has also conducted industry-focused and public-facing awareness campaigns about health care fraud schemes related to the pandemic.

The FBI has arrested over 500 defendants for PPP fraud and seized, recovered, forfeited, or prevented the loss of approximately \$582.7M in PPP funds

The FBI launched initiatives to address a range of fraudulent activity targeting COVID-19 relief programs. As of September 1, 2023, the FBI has opened approximately 746 UI fraud-related cases and 481 EIDL investigations, seizing approximately \$51 million in assets. As of the same date, the FBI has opened over 1,800 PPP related cases and arrested 518 individuals. The FBI has seized, recovered, forfeited, or otherwise prevented the loss of approximately \$582.7 million in PPP funds.

For example, in 2022, a grand jury in the Eastern District of Texas returned an [indictment](#) charging nineteen defendants with conspiracy to commit wire fraud in a case jointly investigated by the FBI and IRS-CI. The indictment alleges that the conspirators fraudulently applied for PPP and EIDL loans and obtained more than \$3.5 million in SBA pandemic relief funds.

In another criminal case jointly undertaken by the FBI and DOL-OIG, a defendant in the Northern District of California was [sentenced](#) in July 2023 to 55 months in federal prison for using more than 136 stolen identities to commit more than \$2.6 million in UI fraud.

In yet another pandemic fraud case jointly investigated by the FBI, IRS-CI, and HSI, a Texas man was sentenced to 180 months imprisonment after [pleading guilty](#) in the Northern District of Texas to fraudulently obtaining \$4 million worth of PPP loans.

Throughout the pandemic, agents and professional staff from the FBI participated in the National Unemployment Insurance Fraud Task Force (NUIFTF) and the International Organized Crime Intelligence and Operations Center (IOC-2). Professional staff also assisted in processing complaints from the National Center for Disaster Fraud (NCDF). The FBI has conducted numerous industry-focused and public-facing awareness campaigns about pandemic relief fraud. These efforts included fraud awareness and training for financial institutions involved in SBA loans as well as agent-focused training on UI fraud.

VIII. U.S. Secret Service

In its continued effort to combat pandemic-related fraud, the U.S. Secret Service (USSS) maintains strong working relationships with federal law enforcement partners, such as SBA-OIG, DOL-OIG, and USPIS, as well as with financial institutions. The USSS continues to use its administrative, civil-judicial, and criminal forfeiture authorities seizing over \$1.4 billion, forfeiting over \$900

million, and remitting over \$400 million in pandemic relief funds to date. The USSS partners with both the U.S. Department of Justice (DOJ) Money Laundering and Asset Recovery Section (MLARS) and the U.S. Treasury Executive Office of Asset Forfeiture (TEOAF).

USSS has seized over \$1.4B, forfeited over \$900M, and remitted over \$400M in pandemic funds

The USSS plays a key role in the DOJ-led NUIFTF. The USSS and our partners continue to investigate pandemic relief fraud. Between March 2020 and November 2023, USSS personnel initiated over 1,500 investigations and over 2,500 investigative inquiries related to SBA loan and UI fraud. For the same reporting period, USSS investigations led to arrests of over 650 individuals for crimes related to SBA loan and UI fraud. For example, three Miami residents were [indicted](#) in November 2023 in the Southern District of Florida for submitting fraudulent PPP loan applications and obtaining \$14.5 million in stolen funds in an investigation USSS jointly worked with SBA-OIG. And 19 defendants were [charged](#) in the Eastern District of Philadelphia for collectively defrauding the PPP, EIDL, and UI programs of more than \$14 million in a case investigated by USSS and six partner agencies.

In addition to investigations and asset recovery, the USSS has provided insights on lessons learned from the pandemic and fraud prevention. In February 2023, the Assistant

Director of the Office of Investigations for USSS also provided [written testimony](#) to the House Committee on Oversight and Accountability in February 2023, to discuss USSS’ response to pandemic fraud.

IRS-CI has initiated ERC fraud investigations involving \$2.9B

IX. IRS Criminal Investigation

Since the start of the of pandemic, IRS Criminal Investigation (IRS-CI) has led and participated in COVID-19 fraud investigations covering a range of fraud typologies, including SBA pandemic loan fraud, counterfeit EIP checks, sale of fraudulent PPE, UI Fraud, and tax-related schemes connected to the pandemic.

Starting in 2023, IRS-CI has seen an increase in fraud related to the Employee Retention Credit (ERC). Bad actors have seized opportunities to personally benefit from ERC claims using IRS Forms of the 940 series (Employer’s Annual Federal Unemployment (FUTA) Tax Return), 941-X (Amended Employer’s Quarterly Federal Tax Return) series, and 7200 (Advance Payment of Employer Credits Due to COVID-19). IRS-CI has continued to conduct data analytics to develop investigative leads focused on ERC fraud.

IRS-CI has been proactive in conducting media and stakeholder outreach to inform taxpayers and tax-professionals of COVID-related fraud and scams. In February of 2024, IRS-CI began hosting a series of educational sessions geared specifically to tax professionals about ERC at its field offices across the country. These sessions are part of a nationwide initiative to ensure that tax professionals have the latest information about ERC claims and understand ERC eligibility criteria.

As of the end of calendar year 2023, CI has initiated 352 investigations involving more than \$2.9 billion in potentially fraudulent ERC claims in tax years 2020 through 2023. Eighteen of the 352 investigations have resulted in federal charges, with 11 convictions and four sentencing with an average sentence of 21 months.

X. United States Postal Inspection Service

Between August 2022 and December 2023, the U.S. Postal Inspection Service (USPIS) generated investigations that have, thus far, led to the arrest of more than 160 people for federal offenses including PPP, EIDL, and UI fraud and involving losses of more than \$283 million.

USPIS worked to bring charges against 160 people for over \$279M in pandemic fraud

For example, in the Eastern District of Virginia, a defendant was sentenced to [42 months in prison](#) in February 2024 for his role in receiving fraudulent EIDL loans using the identities of others. In another case, three individuals were [sentenced](#) for their roles in fraudulently obtaining \$3.5 million in PPP loans.

USPIS has conducted robust COVID-19-related fraud prevention activities through a variety of mediums, including and not limited to, social media postings, public service announcements, and a dedicated COVID-19 [webpage](#) that provides information and prevention tips on various COVID-19 related fraud schemes. USPIS also created internal informational messaging on recognizing and reporting fraud schemes, including those stemming from COVID-19 related fraud, for the U.S. Postal Service’s over 600,000 employees nationwide.

XI. Department of Health and Human Services Office of Inspector General

The COVID-19 pandemic represented a unique opportunity for fraudsters to take advantage of federal health care benefit programs, including Medicare and Medicaid. In response to the pandemic, HHS created two new benefit programs – the Provider Relief Fund (PRF) and Uninsured Program (UIP) – both of which were targeted by individuals and organized criminal groups seeking to commit fraud.

HHS-OIG’s investigations resulted in 290 indictments, 135 criminal convictions, and \$477M in monetary recoveries

HHS-OIG has conducted COVID-19 investigations resulting in 290 indictments, 135 criminal convictions, and monetary recoveries of \$477 million. Agents have leveraged established relationships with United States Attorneys’ Offices and DOJ’s

Medicare Fraud Strike Force to make the greatest possible impact, recover stolen dollars, and bring wrongdoers to justice.

HHS-OIG’s Division of Data Analytics has focused on proactive data analysis to identify potential fraud in the pandemic space. Agents have also worked closely with the Health Resources and Services Administration (HRSA) – which managed the PRF and UIP programs – to highlight bad actors and provide subject matter experts to assist with investigations and prosecutions.

These collaborative efforts have resulted in several impactful cases. For example:

- In March 2023, a Grand Jury in the Northern District of Illinois returned an [indictment](#) charging a Chicago-area lab owner with the fraudulent submission of claims to HRSA for COVID-19 testing, resulting in the receipt of over \$83 million.
- In September 2023, a Los Angeles-area doctor and his coconspirators were [charged](#) with defrauding HRSA’s COVID-19 Uninsured Program. The indictment alleges that the conspirators received approximately \$150 million in payments for services not covered or never provided.
- In January 2024, a California man was [sentenced to ten years in prison](#) for his involvement in operating a laboratory and billing Medicare approximately \$234 million for various lab tests, including COVID-19 tests, despite being excluded from Medicare.

HHS-OIG has received thousands of allegations of pandemic fraud through its [Hotline](https://tips.oig.hhs.gov) (800-HHS-TIPS or <https://tips.oig.hhs.gov>). Agents have conducted outreach to groups such as the Healthcare Fraud Prevention Partnership and National Health Care Anti-Fraud Association to educate public and private insurers about pandemic fraud schemes. HHS-OIG has also worked closely with DOJ's COVID-19 Fraud Enforcement Task Force to bring all possible resources to bear to combat health care fraud involving government programs.

XII. Department of the Treasury Special Inspector General for Pandemic Recovery

The Special Inspector General for Pandemic Recovery (SIGPR) is an IG created by the CARES ACT of 2020 to investigate matters arising from three types of CARES Act loans: (1) Treasury's Direct Loans to air carriers and businesses critical to maintain national security; (2) Treasury's investments into loans made as part of the Main Street Lending Program (MSLP); and (3) PPP loans referred by the PRAC to SIGPR for investigation. Because no principal is due on the Treasury Direct Loans until 2025, and the first 15% principal payments were not due on the MSLP loans until the latter part of 2023 and early 2024, SIGPR developed more than 85% of its case leads proactively.

SIGPR investigations led to 21 arrests, \$11M+ in restitution orders, and nearly \$10M in forfeitures

Between September 1, 2022, and February 28, 2024, SIGPR's investigations resulted in 21 arrests, 21 individuals being charged, and four individuals being sentenced to between one and seven years of incarceration. The sentencings included restitution orders totaling more than \$11 million and forfeiture orders totaling nearly \$10 million. For example, SIGPR, together with the FBI, IRS-CI, and Federal Reserve Board OIG, investigated a convicted felon who fraudulently obtained more than \$2.6 million from the Main Street Lending, PPP, and EIDL programs. The defendant, who was prosecuted in the Middle District of Florida, was [sentenced](#) to more than seven years in federal prison and ordered to pay over \$2.617 million in restitution. SIGPR also partnered with FDIC-OIG and the FBI to investigate several individuals for PPP fraud in a matter initiated by the PRAC. The investigation resulted in fourteen defendants being [charged](#) with fraud in the Northern District of Texas for allegedly filing a total of 29 fraudulent PPP and bank loan applications totaling more than \$50 million.

During the same period, SIGPR opened 28 new investigations and referred 22 individuals to Treasury's Suspension and Debarment Office; seven of which have been debarred to date. SIGPR's investigations have also led to recoveries in the form of early loan repayments totaling more than \$21 million.

SIGPR's Inspector General, Brian Miller, has testified before Congress and engaged in outreach among accountants, lawyers, and other IGs concerning CARES Act fraud. On November 14, 2023, IG Miller

[testified](#) before the Senate Subcommittee on Emerging Threats and Spending Oversight hearing “Examining Federal COVID-Era Spending and Preventing Future Fraud.”

XIII. Treasury Inspector General for Tax Administration

The Treasury Inspector General for Tax Administration (TIGTA) has been involved in numerous Federal criminal investigations since the beginning of the pandemic. During fiscal year 2023, 269 individuals were charged in connection with COVID-19 benefit fraud as a result of TIGTA investigations, bringing the total since March 2020 to 672. Of those individuals, 266 were sentenced and collectively received a total of more than 754 years imprisonment and court-ordered financial restitutions of almost \$159 million. For example, TIGTA investigated a case in the Northern District of Georgia that led to 22 people being [indicted](#) for a \$3.8 million PPP fraud scheme.

XIV. Homeland Security Investigations

Since April 2020, Homeland Security Investigations (HSI) Cyber Crimes Center (C3), Intellectual Property Rights Center (IPRC), Financial Crimes Unit (FCU), and HSI Office of Intelligence representatives have been successfully targeting online fraud schemes and the sale of illicit COVID-19 vaccines and treatments using illicit websites and dark net marketplaces as well as COVID-19-related financial fraud. From August 1, 2022, through September 30, 2023, HSI Special Agents have initiated 174 criminal investigations, made 175 arrests, secured

160 indictments, and 127 convictions while seizing approximately \$7.5 million related to COVID-19 fraud.

Since August 2022, HSI has supported 127 convictions and seized approximately \$7.5M related to COVID-19 fraud

HSI investigations have resulted in indictments for pandemic relief benefit fraud, including PPP and EIDL, as well as UI fraud, counterfeit PPE, and seizures of fraudulent proceeds of those offenses. HSI agents are participating in pandemic relief fraud task forces across the country, as well as the National Unemployment Insurance Fraud Task Force.

XV. Federal Deposit Insurance Corporation Office of Inspector General

Since many pandemic-relief programs are administered through Federal Deposit Insurance Corporation (FDIC) regulated and insured institutions, the FDIC Office of Inspector General (OIG), Office of Investigations (OI) has been actively involved in pandemic-related financial investigations that affect the institutions. The FDIC-OIG’s efforts related to the federal government’s COVID-19 pandemic response have resulted in approximately 196 investigations associated with fraud in pandemic relief programs. Such cases involve fraudulent activity involving theft of funds from Government programs intended to provide financial assistance during the pandemic. Since the beginning of the pandemic, the

FDIC-OIG’s collaborative work in this area has accounted for 77 complaints, 248 indictments or informations, 192 convictions, 257 arrests, and approximately \$271 million in fines/penalties, restitution ordered asset forfeitures, and asset seizures. Some examples of FDIC-OIG-supported matters include:

- [Leader of \\$20M COVID-19 Relief Fraud Ring Sentenced to 15 Years](#)
- [CFO, Controller, Corporate Officers Charged in \\$53 Million Fraud Scheme Involving Pandemic Relief](#)

XVI. Department of Education Office of Inspector General

The U.S. Department of Education Office of Inspector General has been working since 2020 to identify and stop fraud, waste, and abuse of pandemic aid. An investigation with its law enforcement partners led to [the sentencing of a U.S. Army Chief Warrant Officer](#) for leading a “prolific fraud scheme” in which she and others illegally raked in millions of dollars from COVID-19 relief programs and federal student loan forgiveness. The warrant officer submitted more than 150 fraudulent PPP loan applications to the Small Business Administration for herself and others, resulting in more than \$3 million in fraudulent disbursements. Conspirators paid the defendant to submit falsified certifications to discharge of more than a dozen student loans totaling more than \$1 million.

OIG efforts also led to [schools returning Higher Education Emergency Relief Fund \(HEERF\) awards](#), including the owner of a

for-profit, post-secondary school that closed who closed returned more than \$235,000 in HEERF. In another case, a for-profit school was denied additional eligibility in the Federal student aid programs because it improperly accounted for and disbursed HEERF awards to students and did not meet the standards of financial responsibility for administering the programs.

The OIG also continues to distribute fraud awareness materials aimed at helping stakeholders identify and report suspected fraud involving pandemic relief aid. This includes a [digital booklet](#) and a [one-page flyer](#). The materials highlight what education-related coronavirus fraud could look like and provide information on free resources to help identify and report fraud to the OIG. Further, the OIG continues to participate in Federal-State COVID-19 task forces and work groups. These task forces are a collective of Federal and State law enforcement and prosecutive entities combining their investigative power to quickly address fraud complaints and to identify, investigate, and prosecute fraud related to the pandemic. Further, the OIG continues to participate in the PRAC and other Federal-State COVID-19 task forces and work groups.

XVII. Department of Veterans Affairs Office of Inspector General

The U.S. Department of Veterans Affairs Office of Inspector General (VA- OIG) continues to participate in multiple federal criminal investigations related to pandemic fraud. From August 2022 through December 2023, VA-OIG investigations have resulted

in 14 federal indictments or informations, over \$3 million in ordered restitution and forfeiture from defendants, and approximately \$95 million in cost savings and avoidances. During this reporting period, VA-OIG COVID-19-related investigations included alleged bribery and kickback schemes related to fraudulent COVID-19 testing, fraudulent procurement practices regarding personal protective equipment, and fraudulent Paycheck Protection Program (PPP) loans and Economic Injury Disaster Loans (EIDL) received by VA employees. For example, in the Western District of New York, a man was [sentenced to more than 20 years](#) engaging in multiple fraud schemes, including obtaining \$7.4 million by falsely purporting to have N95 masks that he could sell to various entities, including a VA hospital, during the height of the pandemic.

XVIII. Department of Justice Office of Inspector General

The DOJ-OIG has devoted a significant portion of its oversight work since March 2020 to assessing the DOJ's readiness to respond to the COVID-19 pandemic. This has included oversight of pandemic-related grant funding disbursed to state, local, and tribal organizations, as well as the release of a collection of interactive dashboards with data on COVID-19 case trends, testing trends, and deaths due to COVID-19 in BOP-managed correctional facilities.

In January 2021, PRAC stood up a Fraud Task Force to serve as a resource for the Inspector General community by surging investigative resources in those areas where the need is the greatest, currently pandemic

loan fraud. Agents from OIGs across the federal government, including the DOJ-OIG, have been detailed to work on task force cases. These agents have partnered with prosecutors from the Department's Criminal Division, Fraud Section, and United States Attorney's Offices across the country. Since August 2022, the OIG has actively investigated multiple PRAC Fraud Task Force cases, which are in various stages of investigation and prosecution. Some of the subjects in these cases have already been sentenced. For example, on October 23, 2023, a defendant in a PRAC Fraud Task Force case investigated by the OIG was [sentenced](#) to 25 years' imprisonment and ordered pay \$1,120,462 in restitution for using stolen identities to fraudulently obtain PPP and EIDL loans. In addition, DOJ OIG uses proactive data analytics to identify and investigate pandemic-related contract fraud and fraudulent receipt of PPP and EIDL loans by individuals within its jurisdiction.

DOJ-OIG-supported PRAC investigation resulted in defendant sentenced to 25 years' imprisonment for PPP fraud

The DOJ-OIG also has issued several oversight products related to the COVID-19 pandemic, since August 2022. For example, in September 2022, DOJ-OIG issued an Audit of the Management and Coordination of Pandemic-Related Fraud Allegations and Referrals Between the Criminal Division and Executive Office for U.S. Attorneys, which contained recommendations to improve the DOJ's efforts to combat COVID-19 fraud. In addition, since August 2022, the DOJ-OIG has contributed to two joint products with the PRAC Health Care Subgroup.

XIX. Department of Homeland Security, Office of Inspector General

The Department of Homeland Security, Office of Inspector General (DHS-OIG) expanded its COVID-19 Fraud Unit, comprised of experienced special agents, program analysts and data scientists, to develop proactive initiatives to identify COVID-19 fraud and conduct COVID-19 fraud investigations. The DHS-OIG and its investigative partners focused on international fraud rings, public trust employees, and groups of already-incarcerated prison inmates defrauding the government's UI programs.

DHS-OIG investigations have resulted in 87 criminal convictions and over \$20M in recoveries

DHS OIG has opened over 553 high impact investigations, including an inquiry into a Nigerian fraud ring based in Maryland that defrauded several State Workforce Agencies of over \$3.2 million. To date, DHS-OIG investigations have resulted in approximately 126 indictments, 30 criminal informations, 87 convictions, and more than \$21.5 million in recoveries.

In one DHS-OIG case, a Missouri woman was [sentenced to 30 months](#) in federal prison for facilitating the filing of false claims for unemployment benefits by using the stolen identities of incarcerated individuals. In another case, a Connecticut man was [sentenced to four years](#) in prison for fraudulently obtaining Pandemic

Unemployment Assistance by using stolen identities.

XX. Department of Defense Office of Inspector General

The DoD office of Inspector General (DoD-OIG) is responsible for auditing, evaluating, and investigating the programs and operations of the Department of Defense. Congress appropriated approximately \$10.6 billion for the DoD to respond to the COVID-19 pandemic. The DoD-OIG's criminal investigative component, the Defense Criminal Investigative Service (DCIS), initiated investigative projects nationwide to identify fraud in DoD acquisition and health care programs related to the DoD's response to the COVID-19 pandemic.

Since 2021, DCIS's COVID-19 and CARES ACT fraud investigations have led to the arrest of 80 subjects, leading to the conviction of 66 individuals and resulting in approximately 2,300 months of confinement and probation. From FY 2021 through 2023, combined civil and criminal penalties, fines and restitutions totaled \$68,812,391.

DCIS continues to make strides and advances investigating CARES ACT fraud. DCIS HQ components collaborated with experienced field agents to produce the "PPP/EIDL Investigative Guidebook." The guidebook provides DCIS agents suggestions and offers effective tips on how to conduct investigations into PPP and EIDL fraud. During year two, DCIS continued to work collaboratively with other federal law enforcement partners including, the

Department of Justice, the Military Criminal Investigative Organizations (MCIOs) and with CIGIE, providing significantly increased results.

The DoD encourages the use of the DoD Hotline (www.dodig.mil/hotline) to report concerns related to fraud affecting DoD equities, including responses to the COVID-19 pandemic. The hotline provides a confidential, reliable means to report fraud, waste, abuse, and other violations of law that involve the Department of Defense, without fear of reprisal.

XXI. Federal Reserve Board

The Federal Reserve Board has played a vital role in response to the pandemic by enforcing federal consumer protection laws and protecting consumers from abuse. FRB coordinates with U.S. Government Accountability Office; the PRAC, SIGPR, SBA-OIG, and other offices of inspector general to ensure robust oversight of the Board's pandemic response activities, and FRB oversees the CFPB's pandemic response activities through our reviews, to efficiently deploy resources where they are most needed. FRB's Inspector General Bialek is a member of the PRAC Financial Sector Oversight Subcommittee and serves as the vice chair of the PRAC Investigations Subcommittee. FRB's Office of Investigations is dedicated to identifying and investigating potential

fraud related to the lending facilities that are central to the Board's pandemic response. Since the start of the pandemic, our work has resulted in 157 investigations, 93 arrests, 83 convictions, and nearly \$194 million in criminal fines, restitution, and special assessments.

XXII. INTERPOL Washington, the United States National Central Bureau

INTERPOL Washington, the United States National Central Bureau (USNCB), is actively supporting domestic and international efforts to combat COVID-19 related fraud. Conducted in coordination with law enforcement authorities in the U.S. and the 195 other INTERPOL member countries, the USNCB's support activities include, but are not limited to, sharing investigative leads and referrals, participation in multi-national enforcement and interdiction operations, and the production and dissemination of INTERPOL Notices alerting law enforcement authorities to fraud arising from the pandemic.

In October 2023, the USNCB participated in Operation PANGAEA XVI, an INTERPOL-coordinated operation intended to disrupt the activities of organized criminal networks distributing illicit and counterfeit COVID-19 pharmaceuticals and medical supplies online.

LESSONS LEARNED

Our Work is Not Over

The results of the government's collective response to COVID-19 fraud detailed in this report shows the tremendous results possible when agencies work together, particularly given the limited upscaling of investigative and prosecutorial resources. But our work to punish wrongdoers and recoup fraudulently obtained pandemic relief funds is far from over. State workforce agencies continue to provide additional claims data that has yet to be analyzed for leads. The NUIFTF data scientists and analysts continue to make connections from law enforcement data to identify perpetrators of fraud. Funds stolen from pandemic relief programs remain restrained in bank accounts and need to be forfeited. Accordingly, the CFETF strongly supports an extension of the statute of limitations for COVID-19 pandemic benefit fraud, an extension of the data sharing and analysis facilitated by the PRAC, and the necessary resources for CFETF members to continue their impressive work holding fraudsters accountable and recovering stolen funds.

Explore Permanent Coordinated Efforts to Combat Government Benefits Fraud

The response to COVID-19 fraud has made the members of the CFETF keenly aware of the need for a permanent, interagency body to respond to government benefits fraud. The use of stolen and synthetic identities by criminal networks to defraud public benefits programs is a serious and evolving threat to the integrity of federal programs and to the American people those essential programs are intended to help.

There are indicators that the domestic and foreign networks who committed COVID-19 fraud continue to attack federal and state programs, applying criminal skills and tools they acquired during the pandemic to commit fraud. The government is also regularly a victim of cyber-enabled fraudsters in ways beyond identity theft, including by invoice or payment fraud related to federal funds, such as impersonating contractors to fraudulently receive payments or business email compromise. As evidenced by numerous examples around the country, some of which are detailed in this report, domestic violent criminal groups are also turning to identity and government benefit theft. This both heightens the need to improve our response and demonstrates that thwarting government benefit fraud can support efforts to reduce violent crime in our communities.

Fraudsters are increasingly anonymous; detection of the perpetrators and tracing of the money is impossible for a single agency or agent. The benefits from the relationships and data sharing forged in response to pandemic fraud are readily apparent.

The members of the CFETF stand ready to engage with the relevant policy makers to discuss ways to improve our data sharing and a coordinated response to government benefits fraud going forward, including creating an ongoing data-sharing and analytics entity. CFETF members are also eager to discuss the resources needed to address this growing threat; we must have the agents, analysts, and prosecutors in place to analyze data, generate actionable leads, and prosecute these complex cases.