Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs

June 13, 2022

Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs

This Insights Report is based on information gathered by the Pandemic Response Accountability Committee's (PRAC) Identity Fraud Reduction and Redress (IFRR) Working Group and other relevant partners. The report outlines challenges related to addressing identity fraud and highlights actions government agencies can take to both reduce identity fraud and improve victim redress programs.

The COVID-19 pandemic and rapid disbursement of over $5 trillion in federal pandemic response funds created a lucrative opportunity for identity fraud.[1] The Federal Trade Commission (FTC), the primary government agency for assisting victims of identity fraud, received a 2,920 percent increase in identity theft reports related to government documents or benefits fraud in 2020. Moreover, May 2021 reporting from the New York State Comptroller identified an 85 percent increase in identity theft reports compared to the previous year.

Identity fraud seriously impacts victims and can lead to frustrating efforts to reclaim identities, clean up credit scores and financial records, expunge erroneous data, and address tax consequences. In addition to the impacts on unsuspecting victims, significant amounts of taxpayer funds are also put at risk for fraud, as technological advances have made it easier for domestic and international criminals to use stolen or synthetic identities to systematically steal large amounts of government relief funds.[2] While it is too early to compile a total estimate of funds lost to identity fraud during the pandemic, numerous U.S. Department of Justice (DOJ) criminal cases illustrate the complexity and scale of this type of fraud. For example, in 2022, eight individuals were arrested for using the identities of inmates, minors, and others in a scheme to obtain over $25 million in unemployment insurance (UI) benefits. The fraudsters ultimately received over $5 million through the scheme.

Real Victims, Real Impact

According to the Senior Medicare Patrol, two Medicare beneficiaries were recently unable to receive medical care because someone had fraudulently billed Medicare for hospice services using their identities; neither individual was terminally ill nor received hospice services. As a result, one of the two beneficiaries is at risk of not receiving necessary heart surgery because the hospice care appears on his Medicare record. The individual has been unable to remove the hospice care notation from his record and is unable to access his Medicare benefits or receive treatments from his providers.

The second beneficiary hasn't been able to receive home health services after being discharged from the hospital because fraudulent hospice care appeared on his record, too. Similarly, this individual can't correct their Medicare record.

While both issues are being addressed by Medicare contractors, these examples highlight the serious ramifications of identity fraud—in particular, medical identity fraud—on its victims.

[1] While formal definitions differ, the terms "identity fraud" and "identity theft" are often used interchangeably. For example, DOJ does not distinguish between the two in their descriptions. This report uses the term "identity fraud" to better define the crime taking place. However, the verbiage used when referencing other agencies' work in this report reflects the verbiage of that particular agency. As such, both "identity fraud" and "identity theft" will be referenced in this report.

[2] A synthetic identity combines potentially valid personally identifiable information (PII) with accompanying false PII.

To combat these sophisticated identity fraud schemes, the federal government must stand up robust systems to minimize identity fraud in its programs and improve the processes by which victims report identity fraud, obtain their rightful benefits, and restore their identities.

Based on oversight work and recommendations by IFRR Working Group member Offices of Inspectors General (OIG), we have identified specific actions agencies could take to reduce fraud and help victims, such as sharing relevant identity verification data and providing timely assistance to identity fraud victims. These actions are listed in two categories: identity fraud reduction and identity fraud victim redress.

Identity Fraud Reduction-Related Actions

- Conduct data matching to verify identity and eligibility for government programs
- Establish controls or processes that check for duplicate applications or benefits
- Collaborate and coordinate with states and other relevant agencies
- Develop processes to track and analyze fraud cases to identify new patterns or trends
- Strengthen communication about data breaches
- Find opportunities to rely on more forms or methods of identification

Identity Fraud Victim Redress-Related Actions

- Provide a reliable method for identity fraud victims to report the fraud and receive support and regular updates
- Train staff to assist victims of identity fraud so that identity fraud claims are processed efficiently and effectively
- Institute processes to swiftly reinstate benefits or services if they were stopped or not received as a result of identity fraud, and in other appropriate cases

The oversight work by PRAC members discussed in the following pages highlights that while there has been a significant focus on detecting identity fraud, there has not been a similar concerted effort across OIGs to balance this work with examining an agency's ability to help the victims of identity fraud recover their identity and obtain rightful benefits. Following publication of this report, the PRAC and the IFRR Working Group will focus on victim redress processes and claimant satisfaction to bring more attention to the experiences of identity fraud victims.

The actions identified throughout this report were identified primarily through the IFRR Working Group members' responses to survey questions related to identity fraud and redress, and from reports that members provided related to identity fraud. In total, the PRAC received responses from 23 OIGs and reviewed 55 reports related to identity fraud, 16 of which were related to the pandemic (see Appendix A for a full list of submitted reports). These 55 reports included a total of 191 recommendations, many of which related specifically to identity fraud reduction and redress and could be applied across multiple agencies. In addition, information from other government and non-governmental entities relevant to identity fraud reduction and victim redress is also included in this report. Finally, the work completed for this Insights Report complies with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspectors General*, which require that the work adheres to the professional standards of independence, due professional care, and quality assurance to ensure the accuracy of the information presented.

Background

Government benefit programs have long been targeted by criminals using stolen or synthetic identities (see process outlined in Figure 1). With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes. For example, criminals can:

- Submit false applications for loans, credit cards, and government benefits;
- Make fraudulent withdrawals from bank accounts; or
- Obtain other benefits or privileges that criminals might be denied if they were to use their real names.

The Identity Theft and Assumption Deterrence Act (the Act), enacted by Congress in 1998, made identity theft a federal crime. Under federal criminal law, identity theft takes place when someone "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity." Identity fraud, or the unauthorized use of another individual's name, social security number, or date of birth to apply for a credit card is also punishable by fine or imprisonment under the Act. Additionally, the Act mandated that the FTC establish a central complaint system to receive and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

Our review shows that pandemic spending was particularly vulnerable to fraud schemes leveraging stolen or synthetic identities for various reasons. First, Congress made a deliberate decision to make several pandemic relief programs widely available with minimal documentation in an effort to expeditiously get relief into the hands of people who needed it. Likewise, many of the programs were unveiled in crisis conditions without the necessary time to develop effective processes to detect and prevent fraudulent applications. Secondly, outdated and inadequate technology systems at the state and federal level further compounded issues associated with the rapid program roll-out. Additional information about pandemic benefit identity theft and fraud can be found on the PRAC's Identity Fraud webpage.

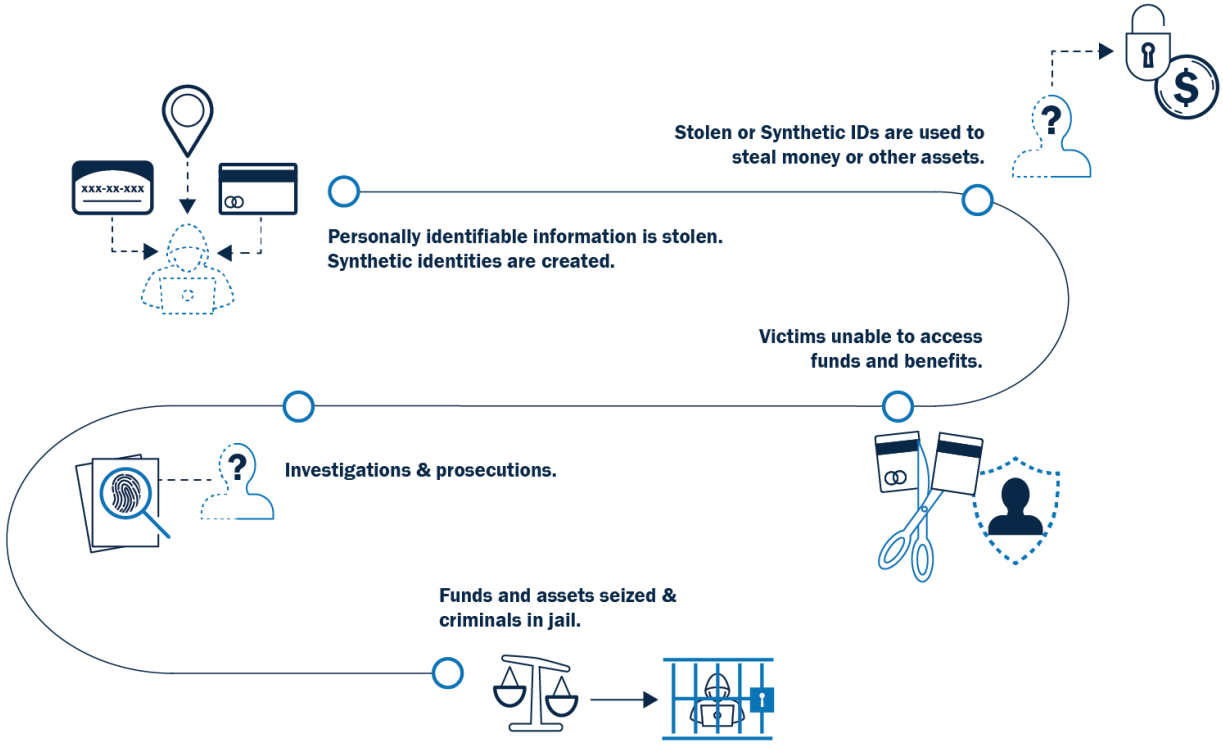
Fast Fact

1.4 million identity theft reports were filed with the FTC in 2020.

Fast Fact

According to the FTC, most stolen identities were used to apply for government documents and benefits in 2020.

Figure 1: Identity Fraud Cycle



Source: PRAC summary presentation of insights from DOJ identity fraud criminal cases.

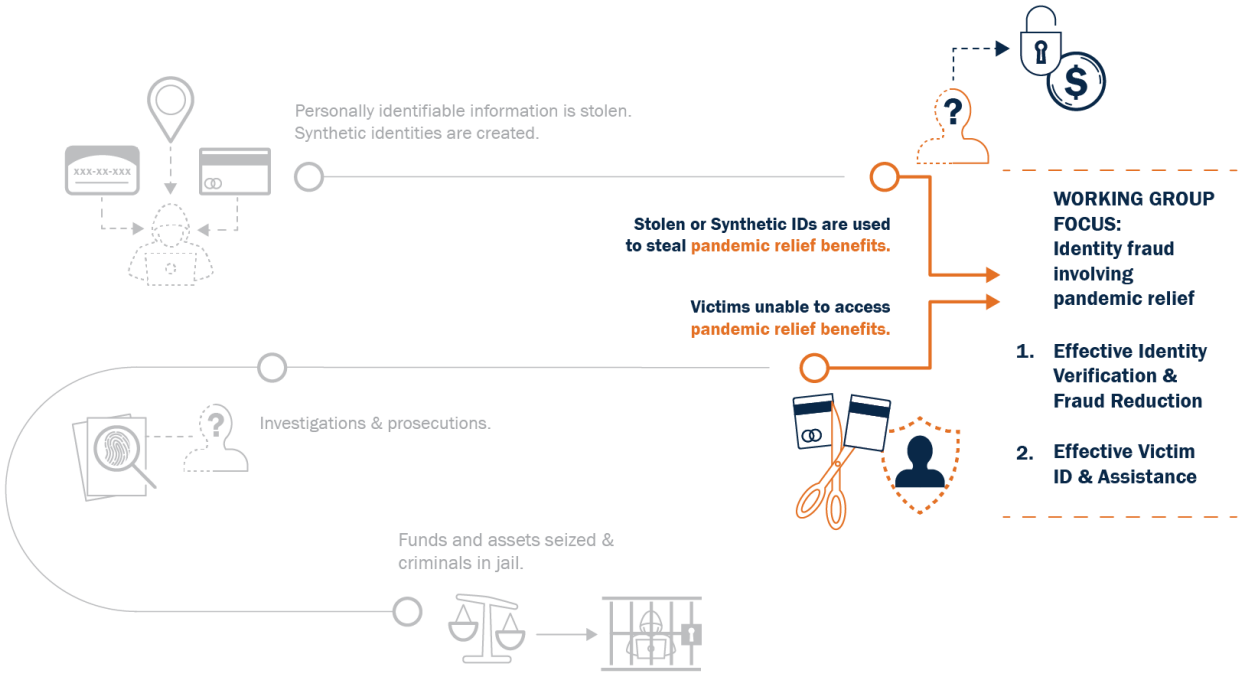
While identity fraud surged in tandem with pandemic relief programs, it is an ever-present threat for American citizens. As such, OIGs have issued reports regarding identity theft and identity fraud both during and prior to the pandemic. Many of these previous findings and associated recommendations can be leveraged by other agencies to reduce identity fraud and better assist victims of identity fraud across the federal government.

Recognizing that fraud was widespread in pandemic relief programs, the government mounted a swift response to uncover fraud schemes and recover the stolen funds. Federal OIGs have been working closely with the Federal Bureau of Investigation and other law enforcement agencies to investigate pandemic fraud. As of April 2022, the PRAC has tracked over 241 indictments and more than 110 convictions related to identity fraud in pandemic programs. While catching these criminals is important for both ensuring appropriate consequences for wrongdoers and deterring such conduct in the future, it would be better in many ways for victims, taxpayers, and federal programs at-large if the government could harden their systems to reduce such exploitation.

IFRR Working Group

To respond to this surge in identity fraud, in July 2021, the PRAC formed the IFRR Working Group, a coalition of OIGs with cognizance over federal agencies targeted by criminals using synthetic identities or stolen identities to access government benefits (See Figure 2 for a depiction of the Working Group's areas of focus).

Figure 2: Areas of Focus for the IFRR Working Group in the Identity Fraud Cycle



Source: PRAC depiction of the IFRR Working Group's Mission based upon Figure 1.

Prevalence of Identity Fraud in Federal Pandemic Programs

Identity fraud has been a common type of fraud across federal pandemic programs—such as the Paycheck Protection Program (PPP), Economic Injury Disaster Loans (EIDL), and Pandemic Unemployment Assistance. The PRAC's January 2022 report on PPP fraud controls, which analyzed a sample of 2020 PPP fraud cases, identified that 21 percent of the cases involved some form of identity fraud. While it is too early to accurately identify the total dollar amount lost to identity fraud during the pandemic, the PRAC's Pandemic Analytics Center of Excellence analyzed hotline data from multiple OIGs to provide insights into the prevalence of identity fraud in pandemic programs.[3] According to their analysis, UI has been particularly prone to identity theft and fraud. **Roughly 95 percent of the 160,000 complaints that have been submitted to the Department of Labor (DOL) OIG hotline during the pandemic (March 2020 to December 2021) mentioned some type of identity fraud**. In many cases the complaints were made by individuals who discovered they had been victimized only after they applied for benefits themselves but were denied because someone had already fraudulently obtained benefits using their identity.

[3] The PRAC and federal OIGs maintain hotlines where individuals can submit information about suspected fraud, waste, abuse, or mismanagement.

Identity Fraud Reduction: Potential Improvements to Reduce Identity Fraud in Pandemic Response Programs

OIGs have completed oversight work during the pandemic that has demonstrated how pervasive identity fraud is in pandemic relief programs and made dozens of recommendations for improvements to reduce identity fraud before it occurs. Many of these findings, along with additional, pre-pandemic findings and recommendations from OIGs in this area, provide broader insights for agencies to consider to better address identity fraud in their programs. While agencies can and should consider incorporating elements of the control activities discussed below, some fraud will still evade appropriately designed controls. It is also essential for agencies to have processes in place to promptly suspend benefits or loans to the fraudster as well as to have processes to adjust their controls once a gap has been identified in order to help prevent similar fraud in the future.

Insight: Conduct Data Matching and Data Linking to Verify Identity and Eligibility for Government Programs

The prevalence of identity fraud in pandemic programs has highlighted the need for better data matching and data linking capabilities.[4] More effective use of data matching or linking could help better detect identity fraud schemes and prevent criminals from using stolen identities to receive benefits illegally. Further, using a whole-of-government approach in data matching to improve identity verification could reduce identity fraud across government programs.

For example, in memorandums issued in February 2021 and June 2021, DOL OIG highlighted four high risk areas within DOL's UI program that could be indicators of possible identity fraud and that could potentially have been mitigated though improved data matching or linking procedures. These areas included:

(1) individuals applying for benefits in multiple states ($12.1 billion in potential fraud);

(2) fraudsters using social security numbers of deceased individuals ($105.2 million in potential fraud);

(3) benefits being provided to federal prisoners or criminals using stolen prisoner identities ($303.4 million in potential fraud); and

(4) fraudsters using suspicious email accounts that hide personal information ($4.5 billion in potential fraud).

When looking at benefits being provided to federal prisoners or criminals using stolen prisoner identities, the Department of Education OIG found in 2011 that fraudsters may target inmates' identities to obtain benefits and recommended that the Department of Education explore the

[4] Data matching refers to comparing two different data sets, such as comparing information from an application for pandemic-related assistance with identification data maintained by another federal agency. Data linking refers to comparing data elements in a single data set, such as analyzing the application data for one pandemic-related assistance program to determine the frequency a single mailing address appears within the data set.

Significant Finding: As of February 2019, SSA OIG found that SSA had improperly paid approximately $46.9 million to 724 beneficiaries who had multiple SSNs and for other reason(s).

feasibility of matching their program applications against data for federal and state inmates to ensure that these inmates and those using the identities of inmates do not obtain these funds. While this recommendation is not directed at UI programs, it does provide insight into the value of matching inmate data against applicant data as a possible fraud control.

Other work completed by federal OIGs can provide insights into possible data matching or linking that could help prevent or reduce identity fraud in federal programs. Table 1 identifies the applicable data matching or linking recommendations previously made by federal OIGs that could be applied more broadly to help prevent or reduce identity fraud in federal government programs. Many of these recommendations are related to the use of social security number data, inmate data, and death data as well as to the use of the Department of the Treasury's (Treasury) Do Not Pay service. In addition, a report issued by the PRAC in January 2022 found that data linking using an internet protocol (IP) address could also be used as a fraud control to reduce identity fraud by identifying an IP address that was used to submit dozens, or even hundreds, of applications for benefits.

Table 1: Types of Data Matching or Linking to Prevent Improper Payments Previously Identified by OIGs

Data Match or Link Type	*Description*	*Agency*	*Examples of Relevant OIG Recommendations or Matters for Consideration*
Social Security Numbers (SSN)	*Fraudsters may attempt to access benefits with an incorrect SSN or may use a stolen SSN with incorrect accompanying information, such as an incorrect date of birth. By matching SSNs with other known records, identity fraud can be reduced.*	Treasury Inspector General for the Tax Administration (TIGTA)	Develop processes and procedures to identify Individual Taxpayer Identification Number or SSN mismatches.
			Evaluate the potential for expanding State Suspicious Filer information sharing agreements to include suspicious or potentially fraudulent business tax returns. [The State Suspicious Filer Program enables participating States to provide the IRS information relating to fraud and identity theft they were identifying]
		Social Security Administration (SSA) OIG	Develop a match to identify and prevent beneficiaries from inappropriately receiving both Old-Age, Survivors, and Disability Insurance and Supplemental Security Income benefits under different SSNs.

Data Match or Link Type	*Description*	*Agency*	*Examples of Relevant OIG Recommendations or Matters for Consideration*
Inmate Data	*Previous OIG work has indicated that fraudsters may target inmates' identities to obtain benefits or loans. Matching application data against available inmate SSN data could help identify instances of possible identity fraud or improper payments.*	Department of Education OIG	Seek a Computer Matching Agreement with the DOJ for its Bureau of Prisons data and explore the feasibility of data matching agreements with State and Federal Trust Territory prison systems to ensure incarcerated persons do not receive Title IV funds for which that are ineligible.
Department of the Treasury's Do Not Pay (DNP)	*Data matching using the Treasury's DNP portal, a centralized data source that can help reduce identity fraud and improper payments in government programs. Treasury's DNP provides this free service to all federal (and some state) agencies.*	SBA OIG	Work with the Treasury to develop a technical solution to enable use of the Treasury's Do Not Pay portal to determine loan applicant eligibility and prevent improper payments before the release of federal funds.
Death Data	*Use of death data may help identify instances where a deceased individual's information has been stolen and is being used to improperly claim or receive benefits.*	Department of Health and Human Services (HHS) OIG	Improve HHS system controls by checking the Enrollment Data Base date-of-death information as close as reasonably possible to the date that card mailing data are sent to the print/mail contractor to ensure that Medicare cards are not mailed to deceased beneficiaries.
		SSA OIG	Add death information to the 48,746 "Death Claim" Numerical Identification System (Numident) records that did not already contain a death entry.

Source: IFRR working group analysis of completed federal OIG reports related to identity fraud.

Insight: Establish Controls or Processes that Check for Duplicate Applications or Benefits

Survey responses and OIG reports emphasized the need for agencies to develop controls that cross-check specific information within their systems for duplicate loans, stolen tax refunds, and more. Examples include individuals who have already received services or benefits or who have received a high number of services or benefits, such as too many tax refunds to a single address or bank account. Too many tax refunds, or other government benefits, being provided to a single address or bank account not just serves as a fraud indicator, but specifically an identity fraud indicator because it can indicate that one individual received the benefits of multiple individuals.

For example, the SSA OIG in 2019 found internal control weakness in the agency's ability to detect when individuals, who had fraudulently obtained multiple SSNs using different names, applied multiple times for benefits. For example, the SSA was unable to detect fraud when individuals were receiving *both* Old-Age, Survivor and Disability Insurance and Supplemental Security Income benefits because of system limitations that prevented matching between these records. As a result, the SSA OIG recommended that the agency develop a process to compare data to identify and prevent beneficiaries from inappropriately receiving both Old-Age, Survivors, and Disability Insurance and Supplemental Security Income benefits under different SSNs.

In another report specifically related to COVID-19 pandemic response programs, the SBA OIG noted that SBA needed to establish review processes to suspend duplicate loans until eligibility is further assessed. Specifically, they recommended that the SBA review duplicate loans to an IP address, email address, business address, or bank account to determine if the loans should be suspended until eligibility is confirmed.

Insight: Collaborate and Coordinate with States and Other Entities Affiliated with Government Benefit Programs

Many federal programs that provide benefits to individuals are managed at the state level. As a result, there are opportunities for criminals to apply in several states to receive multiple benefits using the same stolen identities. Previous OIG work has found that if federal agencies, state agencies, and other organizations can better collaborate, identity fraud could be mitigated. In a February 2021 memorandum, the DOL OIG emphasized the importance of coordination between states and federal agencies, explaining that establishing controls and procedures to allow DOL to communicate with state agencies could help reduce identity fraud. The DOL OIG also noted that states would not be effective at detecting and preventing this type of fraud unless all states consistently perform cross matches. The DOL OIG recommended that DOL establish effective controls, to include data sharing and matching, in collaboration with state workforce agencies, to reduce this type of fraud.

Additionally, during the pandemic, the DOL OIG found that while the Employment and Training Administration had an agreement with the National Association of State Workforce Agencies' (NASWA) UI Integrity Center of Excellence—a national organization that represents all 50 state workforce agencies, the District of Columbia, and U.S. territories—the association was not required to report suspected fraud to DOL or the DOL OIG. The NASWA UI Integrity Center of Excellence allows states to cross match their UI data with other states. Information about suspected fraud within the NASWA's Hub would have likely helped DOL respond to the widespread fraud that occurred in expanded pandemic relief programs. Given that 95 percent of the hotline complaints received by DOL OIG during the pandemic (March 2020 to September 2021) had an identity fraud component, it is likely that the fraud uncovered by NASWA and state workforce agencies also included identity fraud. DOL OIG recommended that the Employment and Training Administration take immediate action to require NASWA to refer information to both DOL and to DOL OIG.

Similar missed opportunities were uncovered in other pandemic relief programs. For example, in their July 2020 report, SBA OIG explained that financial institutions were in a useful position to help the agency identify fraud by confirming the validity of EIDL claimants. **At the time, the SBA OIG had identified 440 financial institutions that had reached out to the SBA to report concerns of potential fraud. However, at the time of the review the SBA did not have a process or partnership**

with financial institutions to review instances of potential fraud. As a result, SBA OIG included a suggested action stating that SBA should create an effective process and method for lenders to report suspected fraud. Similarly, the PRAC's January 2022 report found that identity fraud was one of the key types of fraud present in the PPP and could have likely been mitigated if financial institutions had played a larger role in reporting suspected identity fraud to the SBA to better confirm the validity of borrowers' identities. However, it was not until over a year after the program started that the SBA began to ask all participating PPP lenders to report suspected application fraud (such as identity fraud) to the SBA OIG and the SBA Office of Credit Risk Management.

Prior to the pandemic, OIGs had already completed oversight work recommending additional collaboration with states regarding identity fraud. For example, a report from TIGTA, released in 2015, found that the IRS recognized that additional efforts related to identity fraud were needed. The IRS, at the time, had information sharing agreements in place with several states; however, these agreements only addressed the detection and prevention of individual tax return filing fraud. While beneficial, TIGTA found that this information sharing did not include business tax returns, which increased the risk that the IRS and states would be unable to identify additional types of identity fraud. As a result, TIGTA recommended that the Commissioner, Wage and Investment Division evaluate the potential for expanding State Suspicious Filer information sharing agreements to include suspicious or potentially fraudulent business tax return filings. A more recent report, issued by TIGTA in 2020, found that the IRS has since expanded its information sharing and data matching activities with the Social Security Administration and Treasury's Bureau of Fiscal Service, and the IRS has also established the tax-related identity theft Information Sharing and Analysis Center where state and industry partners share information to help detect, deter, and prevent tax-related identity theft.

Insight: Develop Processes to Track and Analyze Fraud Complaints to Uncover Patterns or Trends

TIGTA and SBA OIG have previously found that tracking identity fraud complaints and data can help identify patterns or trends indicative of fraud schemes and also better manage the identity fraud cases that are handled by the agency. During the pandemic, SBA OIG found there was a significant surge in identity fraud complaints submitted to the SBA. As of January 12, 2021, the SBA had received nearly 81,000 emails in their identity theft email box, as well as other complaints received by their Processing and Disbursement Center. Ultimately, SBA was unable to identify how many complaints they had received related to identity fraud. SBA OIG also found that the agency did not know the exact number of unique identities associated with the stream of complaints received because they did not track this information. As a result, SBA OIG recommended that SBA develop a process to maintain and track all identity fraud complaints. This recommendation is consistent with previous work from TIGTA conducted roughly a decade ago which found that, at the time, the IRS did not use the data collected from identity theft cases to detect or prevent future fraud and recommended that IRS develop processes for data to be tracked and analyzed for trends and patterns. Since TIGTA made those recommendations, a 2020 report noted that the IRS has taken steps to improve its analytical capabilities, such as using data to identify and confirm individual identity theft tax returns, as well as using data to evaluate the need for changes to the identity theft detection filters that are to be put into place for the following filing season.

Insight: Strengthen Communication Surrounding Breaches

Based on IFRR survey results and previous OIG work, there may also be opportunities for agencies to educate and inform service providers and individuals about how to communicate potential widespread identity theft and fraud within a program. Agencies should identify opportunities to strengthen two-way communication with the organizations they work with to make them aware of cyber breaches quickly and then share information with other organizations that the agency works with as well as affected individuals as soon as possible. By doing so, the damage caused by identity theft data breaches could be minimized.

OIGs have emphasized the importance of ensuring service providers are aware of reporting requirements to quickly respond when PII breaches occur. For example, HHS OIG found in 2018 that State Medicaid agencies and their contractors have established procedures to respond to breaches, including notifying affected individuals. However, although the Centers for Medicare and Medicaid Services (CMS) guidance advises states to notify CMS of breaches, HHS OIG found that most states do not routinely do so. As such, the HHS OIG recommended that HHS reissue guidance to states about reporting Medicaid data breaches to them and clarifying its expectations regarding Medicaid data breaches. The OIG emphasized that this information would allow CMS to identify Medicaid contractors that have experienced breaches across multiple states and improve their ability to identify and share best practices for protecting Medicaid beneficiaries and programs. CMS concurred with the recommendation and took steps to issue updated guidance to states.

Insight: Find Opportunities to Rely on More Robust Forms or Methods of Identification

The federal government often relies on specific identifying information to confirm that individuals are who they say they are, and historically, the federal government has used an individual's SSN to verify their identity. However, this reliance on specific or singular identifying information allows fraudsters to target this particular piece of data to exploit an individual's identity and makes it easier for fraudsters to use a stolen, or synthetic, identity to obtain government benefits. For example, with data breaches making SSNs more available to fraudsters, the use of only this identifier increases the risk of identity fraud. While the IRS still uses SSNs to identify an individual, it has recently incorporated the use of a Personal Protection Identification Number (IP PIN) to verify identity, which essentially creates a dual-factor identity validation process so if an SSN was exposed during a breach, a bad actor would not be able to access benefits unless they also knew the correct IP PIN.

As the Government Accountability Office (GAO) explained in a 2017 report, SSNs were not originally intended to be used as personal identifiers outside of SSA programs. However, because SSNs were both universal and unique, government agencies and private sector entities began to, and continue to, use them to identify individuals. GAO emphasized that because data breaches pose a persistent threat across the government, the government has attempted to decrease the use of individual's SSNs within these agencies. As of 2017, all Chief Financial Officer Act agencies reported that they were successfully reducing the collection, use, and display of individual's SSNs, and ultimately reducing the threat of individual's exposure to identity theft.[5] The strategies these agencies

[5] The Chief Financial Officer Act gave OMB new authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting. See here for full list of agencies listed in the Act.

employed included developing and using alternate identifiers, removing SSNs from printed forms and other physical displays, filtering e-mail to prevent unencrypted transmittal of SSNs, and more. However, the Office of Management and Budget has yet to adopt effective practices to guide and monitor agency efforts to reduce SSN use, which the GAO cites as a significant impediment to reducing the risk that fraudsters may use SSNs to commit identity theft.

Despite the absence of specific guidance from the Office of Management and Budget, continued progress has been made in this area. For example, as of 2019, in response to a 2015 federal law, the CMS has fully replaced SSN-based claim numbers on Medicare cards with a unique, randomly assigned Medicare Beneficiary Identifier to better protect Medicare beneficiaries from identity theft. This reflected findings from HHS OIG roughly a decade ago that resulted in the OIG recommending that CMS develop a method for reissuing identification numbers to beneficiaries affected by medical identity theft. Previously, CMS had difficulty assigning new beneficiary numbers because they were linked to an individual's SSN. Now, when an individual's Medicare Beneficiary Identifier is compromised, CMS can issue a new Identifier without impacting an individual's social security benefits or other government benefits.

Other efforts in this area have also been made. Over a decade ago the IRS began issuing IP PINs, a personal six-digit number to add an additional layer of protection to confirmed victims of identity theft. As of 2014, the IRS expanded IP PIN issuance to an opt-in program which allowed anyone who wanted additional identity protection to use IP PINs. The opt-in program was initially only available for individuals in locations with the highest per capita rates of identity theft. Since then, the program has continued to expand. The implementation of the Taxpayer First Act in 2019 required the opt-in program to be available to all individuals in the United States by July 1, 2024. Although, a TIGTA report from September 2020 identified low participation in this program. IRS management believes that actions taken in Processing Year (PY) 2020 increased taxpayer awareness of the opt-in program because the number of taxpayers who successfully passed authentication and obtained an IP PIN nearly doubled to 49,296 in PY 2020 over PY 2019.

Identity Fraud Redress: Gaps in Agencies' Identity Fraud Victim Redress and Assistance Resulted in Victims Not Obtaining Needed Benefits or Having Difficulty Correcting Their Identity Information

After an individual's identity has been used to fraudulently obtain benefits, the process to restore their identity and resolve the fraud can be time consuming and difficult. If the matter is not resolved in a timely manner, victims have difficulty obtaining their rightful benefits, which could result in distressed families, homelessness, and other adverse outcomes.

Likewise, failure to clear up stolen and misused identity information can cause victims to receive a bad credit rating, to have their "delinquent" accounts reported to a collection agency, to have their tax returns flagged for non-payment of taxes on benefits they never received, or to have faulty

information in their medical records if the fraud was related to medical care or prescription drugs. For example, pandemic-related complaints submitted in 2020 to the Identity Theft Resource Center, a non-profit organization that aims to minimize the impact of identity compromise, showed that victims struggled to meet their financial obligations, such as securing housing, paying bills, and avoiding debt. **Forty percent of these victims were unable to pay their routine monthly bills.** Additionally, of those surveyed, 24 percent were denied unemployment benefits because someone applied using their information and 21 percent had their Economic Impact Payment stolen.

Based on the survey responses provided from working group members as well as previous audit work conducted by PRAC OIGs, there is a consistent gap across agencies in their ability to properly redress identity fraud and provide support for the victims of identity theft and fraud. This is especially concerning as the FTC reported that consumers reported losing more than $3.3 billion to fraud in 2020, with government documents or benefits fraud topping the list of types of identity fraud reported to the agency that year.

Current Victim Redress Process for Federal Benefits

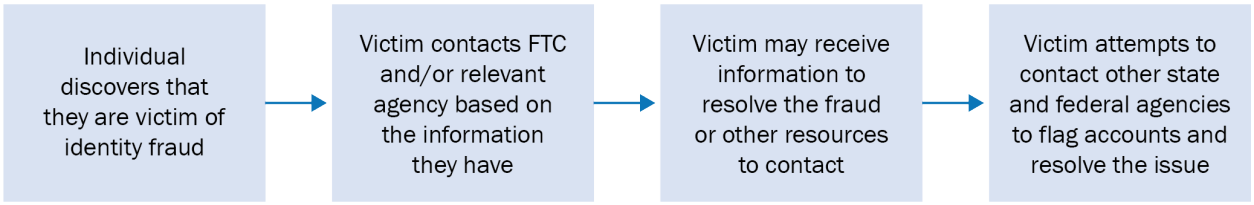
Every case of pandemic benefit identity fraud has three potential victims: the taxpayers, the person whose identity is fraudulently used, and the person whose benefits are fraudulently stolen. In some cases, the second two victims overlap, but not always. For example, an individual's identity could be stolen and used to apply for UI benefits, even though they never lost their job. Identity fraud reduction, discussed above, focuses on the taxpayers as victims and on the investigation and prosecution of individual or groups of fraudsters. The following section focuses on the victims whose benefits are stolen, or whose identity is stolen and used to commit the fraud, and opportunities for government agencies to improve the redress process for assisting those victims to obtain their rightful benefits, to repair the damage caused by misuse of their identity, or both. The victim redress process highlights a significant equity issue because individuals may not be equipped to complete these steps if they have limited understanding of the process or limited resources. While they can work with non-governmental agencies such as the Identity Theft Resource Center, the government resources in this area are not robust. The decentralized nature of the government's identity fraud redress process ultimately places the burden of resolving identity theft and identity fraud on the victims.

Currently, the victim redress process largely relies on victims of identity fraud to take the necessary actions to seek recovery and to be the drivers of the process (see Figure 3).[6] For example, the FTC's IdentityTheft.gov website—the government's central identity fraud reporting website—is designed as a self-service website where victims can enter their complaint and obtain resources, points of contact, and recovery action plans depending on the type of identity fraud reported (i.e. credit card, medical, unemployment, etc.). The recovery plan is essentially a checklist of actions the victim can take, such as contacting credit bureaus.[7] The FTC's website, however, neither shares collected claimant data with relevant government and non-governmental entities or agencies

[6] This report focuses on victims of identity fraud for government benefits. While a victim can also reach out to the FTC through its website if they have been a victim of identity fraud for commercial services, such as having a fraudster open a credit card in their name, those victims may also contact the applicable commercial entity, such as the credit card company, to resolve the issue and may never end up contacting the FTC.
[7] A sample identity theft recovery plan can also be found on the DOJ website.

nor coordinates victim services across the government.[8] Additionally, the FTC does not track the victim's recovery progress or the status of their complaint.

Figure 3: Current Federal Benefit Victim Redress Process—Restoring Identity

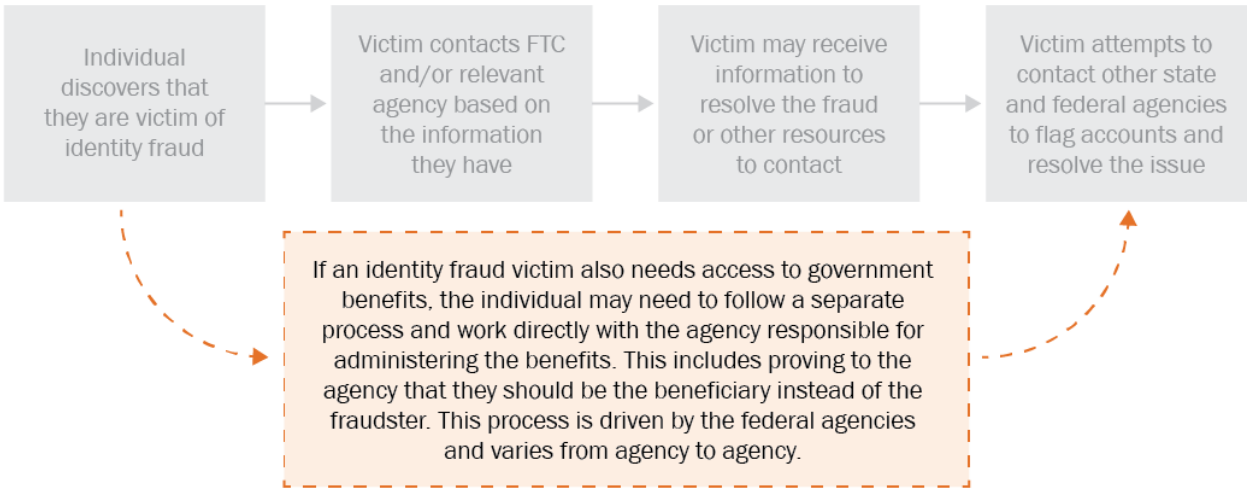


Source: PRAC presentation of information obtained from the FTC regarding its victim assistance program.

As noted above, a victim could have had their identity stolen and follow the process in Figure 3, but if that individual also needs access to benefits, they may have to initiate a completely separate process with the responsible agency to obtain needed benefits.

If an individual's identity is stolen and used for federal benefits that the victim needs, such as UI benefits or a PPP loan for their business, the process to remedy the situation and obtain benefits can be even more taxing and difficult and often varies by agency (see Figure 4). Regarding identity fraud during the pandemic, early evaluations from identity fraud redress experts have found that overburdened and often unresponsive systems have made it difficult for victims to report issues and receive assistance.

Figure 4: Current Federal Victim Redress Process—Receiving or Reinstating Benefits After Fraud



Source: PRAC presentation of information obtained through identity fraud panel host by IFRR Working Group and related OIG work.

[8] The FTC has previously worked with the IRS to develop a process where a victim of tax identity theft can report to the IRS through an electronic form on the FTC's identitytheft.gov website. FTC officials stated that with their current levels of available funds and workforce, replicating this system with other agencies or non-governmental entities is likely not possible.

To date, only a small number of OIGs that are members of the PRAC (TIGTA, HHS OIG, SBA OIG, SSA OIG, and Department of Veteran Affairs OIG) have conducted oversight work to assess the effectiveness of identity fraud victim redress within their agency. Many PRAC OIGs cited fraud investigative units and prosecutions as their main focus for addressing identity fraud. More needs to be done to understand and assess victim redress processes. As such, this will be a focus area for the IFRR Working Group moving forward.

In the interim, the completed work by OIGs provides some initial insights into identity fraud victim redress programs administered by the federal government and elements a federal agency may want to consider including in its program. For example, agencies should develop programs or processes to make it easier for victims to quickly report identity fraud, track those reports, respond to victims in a timely manner, provide support and regularly communicate with victims of identity fraud, and train staff to properly identify and mediate identity fraud cases.

Insight: Provide Support and Regular Updates to Victims of Identity Fraud

Agencies should provide an easy and reliable method for victims to report identity fraud, provide timely updates to those victims regarding their cases, and proactively reach out to potential victims of identity fraud when there is an indication that identity fraud has occurred. This approach can help reduce the individual burden on identity fraud victims and allow them to have a better understanding of what occurred, how to remedy their current situation, and how to better protect themselves in the future.

While the FTC is the lead federal agency for providing assistance to victims of identity theft and fraud, according to the agency the program does not provide feedback or additional support, beyond supplying initial resources, because it is designed as a self-service website. To get feedback or updates, victims must rely on the applicable agencies to resolve their identity fraud issues. This process often differs by agency and has room for improvement as OIGs have previously emphasized the importance of focusing on the support to victims of identity fraud.

In their May 2021 report on identity theft in EIDL programs, the SBA OIG found that because SBA did not track all identity fraud complaints, they could not contact potential identity fraud victims to assist with remediating the fraudulent activity. Ultimately, no systematic process existed for victims of identity theft to report the issues to SBA or for the agency to reach back out to victims to provide information such as updates on the status of their cases. Identity theft victims often reached out multiple times and reported having difficulties in speaking with officials who could help them resolve their issues. The SBA OIG recommended that SBA (1) develop a process to maintain and track all identity theft complaints; (2) develop a process to provide status updates to each complainant alleging identity theft; and (3) complete and formalize a process to restore identity theft victims to their condition prior to the fraud.

Real Victims, Real Impact

At a panel held by the IFFR Working Group in March of 2022, identity fraud reduction experts emphasized that identity fraud victims are often unsure of which agencies they need to report the fraud to when they discover they are a victim and that these victims are frequently not provided any updates or information related to their case.

In a 2020 report, TIGTA found that the IRS did not notify the heirs of deceased individuals that the decedent's personal information had been fraudulently used. The IRS explained that the emotional burden of notifying decedents' heirs outweighs any benefit, but TIGTA believed that the notification from the IRS may be the only way family members are alerted to this crime and would allow them to take the steps needed to protect their deceased family member's personal information. In the same report, TIGTA identified that the IRS did not notify the parents and legal guardians of dependents when their Taxpayer Identification Numbers were used by other individuals to gain employment. TIGTA, which initially identified this issue in a 2017 report, emphasized that this has a negative impact on dependents (who do not have active tax accounts because they are claimed on other's tax returns) and noted that this failure to notify parents and legal guardians prohibits legal guardians from taking proactive steps to protect their dependent's identity. As a result, TIGTA recommended that the IRS develop a process to identify and notify parents and legal guardians when a dependent's taxpayer identification number is used to fraudulently gain employment. However, in both 2017 and 2020, the IRS disagreed with the recommendation and stated they do not intend to notify individuals without active tax accounts. TIGTA continues to believe that without this notification, parents and legal guardians cannot take the same proactive steps the IRS suggests when an adult's taxpayer identification number is identified as being used to fraudulently obtain employment.

In 2021, TIGTA reported that the IRS did develop an outreach strategy to assist taxpayers affected by the increase in unemployment identity theft due to the COVID-19 pandemic. The IRS issued guidance to states in December 2020 regarding the issuance of Form 1099-G, *Certain Government Payments*, which is used to report unemployment compensation. The guidance states that no Form 1099-G should be issued to known victims of unemployment fraud as it would impact victims' tax returns. Guidance issued by the IRS to victims of unemployment identity fraud in January 2021 states that individuals who believe they are a victim of unemployment identity theft and received a Form 1099-G should contact their respective State to request a corrected Form 1099-G. Taxpayers who are unable to obtain a timely corrected Form 1099-G are instructed to file an accurate tax return and not report the fraudulent unemployment income on their tax return. In the context of our review, TIGTA's reporting demonstrates that much of the work to resolve identity fraud still often falls on victims of identity fraud.

Insight: Train Staff to Assist Victims of Identity Fraud Efficiently and Effectively

Previous work conducted by IFRR partners has also demonstrated that properly trained staff are key to identity fraud redress. Staff who are trained to assist identity fraud victims and handle their complaints can more appropriately respond to unique and challenging problems that may occur with an identity fraud case as well as resolve issues caused by the fraud, such as reinstating government benefits. The federal government has already made some process in this area. For example, since 2008, the IRS has had an Identity Protection Specialized Unit in place as part of its strategy to reduce taxpayer burdens caused by identity fraud. However, there is still room for improvement at the IRS, and many other agencies have not been as proactive.

A 2015 report from TIGTA found that it took **the IRS an average of 278 days to resolve tax accounts of identity theft victims**. TIGTA recommended that the IRS develop a comprehensive

identity theft training course to ensure that assistors are capable of handling complex cases. That same year, the IRS centralized its identity theft functions into an Identity Theft Victim Assistance Directorate to improve the taxpayer's experience working with the IRS to resolve their identity theft issues. Both in 2017 and 2020, TIGTA confirmed that this centralization reduced the length of time that the IRS took to resolve cases and the number of errors employees committed while resolving cases. However, the IRS faced new challenges handling identity theft cases during the pandemic. In December 2021, the IRS told taxpayers that the pandemic caused identity theft case inventories to increase dramatically and that it was taking the agency an average of 260 days to resolve identity theft cases.

Insight: Swift Reinstatement of Benefits and Services

When identity fraud occurs, the victims are often unable to access their benefits. This is particularly concerning for pandemic response programs or similar emergency or disaster relief programs, as these benefits may be essential to the stability and well-being of these victims. For example, an individual who has applied for unemployment benefits may be unable to support, feed, or house their family because a criminal already used their identity to apply for benefits. As such, processes should swiftly resolve fraud claims and reinstate benefits or services if those benefits or services were suspended or denied as a result of identity fraud. Previous findings and recommendations from OIGs have emphasized the importance of allowing victims access to necessary benefits while the related identity fraud is resolved.

Allow Victims to Retain Services | Agencies should re-evaluate their practice of suspending services in appropriate cases when there is an indication of identity fraud. The victim of identity fraud may be in dire need of these benefits or services. Over a decade ago, HHS OIG emphasized the need for continued services while a fraud claim is processed. In a 2012 report, the OIG recommended that CMS develop a method for ensuring that beneficiaries who are victims of medical identity fraud retain access to critical medical services. The OIG suggested the CMS insert an indicator in the beneficiary claim record that could allow for payment of legitimate claims for victims of medical identity theft.

Real Victims, Real Impact

According to panelists at the IFRR's Identity Fraud Redress panel in March 2022, victims of identity fraud often struggle to access their benefits following the identity fraud because fraudulent information is now associated with their identity. "Detangling" the fraudulent information from the legitimate information can often be difficult and delay victims receiving their benefits.

Restore or Reissue Victim Identity Information or Benefits| If an identity fraud victim's benefits are suspended, agencies must have processes in place to swiftly restore or reissue the benefits to the victim.

During the pandemic, SBA experienced an increase in identity theft within the EIDL program. In a 2021 report the SBA OIG stated that **as of January 31, 2021 $1.1 billion in loans that were disbursed based on false application information (some of these likely related to identity theft) had been recovered**. However, at the time of this report, SBA did not have a process to resolve credit-related issues for identity theft victims. For example, for loans that were disbursed but not fully recovered, SBA did not have a process to cease billing fraudulent loans to the victims, prevent collection actions, and release the victim from the loan liability. Based on these

findings, the SBA OIG recommended that SBA formalize a process to restore identity theft victims to their condition prior to the fraud.

The Way Ahead for Identity Fraud Reduction and Redress: A Focus on Victims' and Claimants' Experiences

As described above, PRAC OIGs have already completed important work to identify and reduce identity fraud in pandemic relief programs. Some of this work has also highlighted the often-frustrating experiences of identity fraud victims and the real harms they encounter.

The work outlined in this report and in additional reports posted on the PRAC's website, show that, to date, much of the PRAC's oversight work has centered on mitigating, investigating, and recovering fraudulent payments. A review of these reports also shows that many fraudulent pandemic relief payments were obtained using stolen or synthetic identities. Each investigation or audit helps pinpoint methods used to fraudulently obtain benefits and highlights measures agencies can adopt to reduce fraudulent or otherwise improper payments. If successful, agencies can continuously improve their fraud reduction controls.

To bring more attention to the experiences of identity fraud victims and to help ensure that fraud reduction controls strike an appropriate balance between preventing fraudulent payments and allowing legitimate claimants to receive government benefits, the PRAC and the IFRR Working Group plans to increase its focus on victim redress processes and claimant satisfaction.

Greater attention on how individuals and businesses experience relief programs will improve the overall federal customer experience, which is at the heart of how the government interacts with its citizens, particularly when responding to major disasters.

PRAC OIGs will continue to look for fraud, waste, and abuse while working to ensure that vital financial relief reaches the individuals and businesses it was intended to help. PRAC OIGs' identity fraud reduction and redress reports will continue to be posted to PandemicOversight.gov and relevant reports and investigations can also be found on the PRAC's Identity Fraud webpage.

Acronym List

CMS	Centers for Medicare and Medicaid Services
COVID-19	novel coronavirus-2019
DNP	Department of the Treasury's Do Not Pay Center
DOJ	Department of Justice
DOL	Department of Labor
EIDL	Economic Injury Disaster Loan
FTC	Federal Trade Commission
GAO	Government Accountability Office
HHS	Department of Health and Human Services
IFRR	Identity Fraud Reduction and Redress working group
IP	Internet Protocol
IP PIN	Identity Protection Personal Identification Number
NASWA	National Association of State Workforce Agencies
OIG	Office of Inspector General
PII	Personally Identifiable Information
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
SSA	Social Security Administration
SSN	Social Security Number
The Act	The Identity Theft and Assumption Deterrence Act
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
UI	Unemployment Insurance

Appendix A: List of Identity Fraud Reports Evaluated

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Department of Labor	Alert Memorandum: ETA Does Not Require the National Association of State Workforce Agencies to Report Suspected UI Fraud Data to the OIG	July 1, 2021	●		●			●		
	Alert Memorandum: The Employment and Training Administration Needs to Issue Guidance to Ensure State Workforce Agencies Provide Requested Unemployment Insurance Data to the Office of Inspector General	June 16, 2021	●		●	●				
	COVID-19: States Struggled to Implement Cares Act Unemployment Insurance Programs	May 28, 2021	●		●					
	Alert Memorandum: The Employment and Training Administration (ETA) Needs to Ensure State Workforce Agencies (SWA) Implement Effective Unemployment Insurance Program Fraud Controls for High-Risk Areas	February 22, 2021	●		●	●		●		
	COVID-19: States Cite Vulnerabilities in Detecting Fraud While Complying with the CARES Act UI Program Self-Certification Requirement	October 21, 2020	●		●					
	COVID-19: More Can Be Done to Mitigate Risk to Unemployment Compensation Under The CARES Act	August 7, 2020	●		●					

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Department of Labor (cont.)	Alert Memorandum: The Pandemic Unemployment Assistance Program Needs Proactive Measures to Detect and Prevent Improper Payments and Fraud	May 26, 2020	●		●					
	CARES Act: Initial Areas of Concern Regarding Implementation of Unemployment Insurance Provisions	April 21, 2020	●		●					
Department of Education	Fraud in Postsecondary Distance Education Programs (fraud rings) Reporting Change	August 21, 2020	●							
	Investigative Program Advisory Report: Distance Education Fraud Rings	September 26, 2011	●			●				
Department of Health and Human Services	The Majority of Providers Reviewed Used Medicare Part D Eligibility Verification Transactions for Potentially Inappropriate Purposes	February 11, 2020				●				
	CMS's Controls Over Assigning Medicare Beneficiary Identifiers and Mailing New Medicare Cards Were Generally Effective but Could Be Improved in Some Areas	January 13, 2020	●			●				
	States Follow a Common Framework in Responding to Breaches of Medicaid Data	October 16, 2018	●				●			
	OCR Should Strengthen Its Oversight of Covered Entities' Compliance With the HIPAA Privacy Standards	September 28, 2015	●							

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Department of Health and Human Services (cont.)	OCR Should Strengthen Its Follow-up of Breaches of Patient Health Information Reported by Covered Entities	September 28, 2015	●							
	CMS Response to Breaches and Medical Identity Theft	October 1, 2012	●	●			●			
Government Accountability Office	Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display	July 25, 2017		●			●			
Pandemic Response Accountability Committee	Small Business Administration Paycheck Protection Program Phase III Fraud Controls	January 21, 2022	●		●			●		
Small Business Administration	SBA's Handling of Identity Theft in the COVID-19 Economic Injury Disaster Loan Program	May 6, 2021		●	●				●	●
	Inspection of Small Business Administration's Initial Disaster Assistance Response to the Coronavirus Pandemic	October 28, 2020	●		●	●				
	Serious Concerns of Potential Fraud in Economic Injury Disaster Loan Program Pertaining to the Response to COVID-19	July 28, 2020	●		●			●		

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Small Business Administration (cont.)	Memorandum: Key Recommendations Based on Lessons Learned from Prior COVID-19 Economic Injury Disaster and Paycheck Protection Program Loan Programs	December 23, 2020	●		●	●				
Social Security Administration	The Social Security Administration's Processing of Misuse Allegations of Individual Representative Payees	June 14, 2021		●						
	The Social Security Administration's Implementation of iPaySSA	July 30, 2020	●							
	The Social Security Administration's Controls for Identifying Potentially Fraudulent Internet Claims	September 16, 2019	●			●				
	Follow-up: Individuals Who Inappropriately Received Benefits Under Multiple Social Security Numbers	April 25, 2019	●			●				
	Verifying the Identities of Individuals Who File Internet Claims	November 7, 2018	●							
	Unauthorized my Social Security Direct Deposit Changes Through May 2018	September 27, 2019	●							
	Improper Use of Elderly Individuals' Social Security Numbers	January 3, 2017	●							
	Unauthorized Direct Deposit Changes through my Social Security	September 23, 2015	●							

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Social Security Administration (cont.)	The Social Security Administration's Authentication Risk Assessment for the Internet Social Security Number Replacement Card Project	May 15, 2015	●							
	Numberholders Age 112 or Older Who Did Not Have a Death Entry on	March 4, 2015	●			●				
	Follow-up: Individuals Receiving Benefits Under Multiple Social Security Numbers At Different Addresses	January 13, 2012	●							
Treasury Inspector General for Tax Administration	Implementation of Tax Year 2020 Employer Tax Credits Enacted in Response to the COVID-19 Pandemic	June 9, 2021	●		●					
	Assessment of Processes to Verify Tentative Carryback Refund Eligibility	June 2, 2021	●		●					
	Implementation of Economic Impact Payments	May 24, 2021	●		●					
	Interim Results of the 2021 Filing Season	May 6, 2021		●	●				●	
	Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts	October 21, 2020	●							

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Treasury Inspector General for Tax Administration (cont.)	Taxpayer First Act: Implementation of Identity Theft Victim Assistance Provisions	September 10, 2020		●					●	
	Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives	July 10, 2020	●					●		
	Improved Procedures Are Needed to Prevent the Fraudulent Use of Third-Party Authorization Forms to Obtain Taxpayer Information	August 27, 2018	●							
	Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft	August 20, 2018	●							
	The Number of Employment-Related Identity Theft Victims is Significantly Greater Than Identified	June 20, 2017	●	●		●			●	
	Centralization of Identity Theft Victim Assistance Reduced Case Closure Time Frames and Tax Account Errors	June 6, 2017		●						
	Process Are Not Sufficient to Assist Victims of Employment-Related Identity Theft	August 10, 2016		●						
	Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection	December 11, 2015	●							

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Treasury Inspector General for Tax Administration (cont.)	Improvements Are Needed in the Identity Protection Specialized Unit to Better Assist Victims of Identity Theft	October 27, 2015		●					●	
	Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection	September 9, 2015	●			●		●		
	Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft	April 24, 2015	●							
	Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds	March 20, 2015		●					●	
	Case Processing Delays and Tax Account Errors Increased Hardship for Victims of Identity Theft	September 26, 2013	●	●						
	Stolen and Falsely Obtained Employer Identification Numbers Are Used to Report False Income and Withholding	September 23, 2013	●							
	Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds	September 20, 2013	●							
	There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting from Identity Theft	July 19, 2012	●							

Office of Inspector General	*Report Title*	*Date Issued*	*Identity Fraud Reduction*	*Identity Fraud Redress*	*Pandemic-related*	*Data Matching or Linking*	*Breaches*	*Coordination with Other Entities*	*Staff to Support Victims*	*Track and Analze Fraud Complains*
Treasury Inspector General for Tax Administration (cont.)	Most Taxpayers Whose Identity Has Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service	May 3, 2012		●					●	
United States Postal Service	The Role of the Postal Service in Identity Verification	May 16, 2022	●	●	●					
	Passport to Excellence	April 11, 2016	●							
	e-Government and the Postal Service - A Conduit to Help Government Meet Citizens' Needs	January 7, 2013	●							
Department of Veteran Affairs	VBA's Fiduciary Program Needs to Improve the Timeliness of Determinations and Reimbursements of Misused Funds	July 21, 2021		●						

PRAC point of contact:

Amanda Seese
Associate Director of Oversight and Accountability
Amanda.Seese@cigie.gov

For more information about the specific OIG reports referenced in this Insights Reports, please reach out to the applicable point of contact identified on our website.

Visit our website at:

PandemicOversight.gov

Follow us on social media

@COVID_Oversight

Report fraud, waste, abuse, or misconduct:

To report allegations of fraud, waste, abuse, or misconduct regarding pandemic relief funds or programs, please go to the PRAC website at PandemicOversight.gov.

A Committee of the
Council of the Inspectors General
on Integrity and Efficiency