



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

441 G STREET, NW, SUITE 1517, WASHINGTON, DC 20548

## MEMORANDUM

Following the coronavirus outbreak, Congress created the Pandemic Response Accountability Committee (PRAC) in March 2020 to support and coordinate independent oversight of what is now more than \$5 trillion in pandemic-related programs and spending. The PRAC, with the support of its Office of Inspector General (OIG) partners, is charged with examining whether pandemic funds were used for their intended purpose and the extent of the fraud, waste, and abuse associated with these relief funds. Through collaborative oversight work, the PRAC and our OIG partners have identified identity fraud as a critical issue across multiple pandemic programs, such as the Pandemic Unemployment Assistance program and the Paycheck Protection Program, among others. In programs like these, federal agencies relied on self-certification and lowered guardrails to disburse pandemic relief funds at record speed. What millions of Americans saw as relief from the economic challenges caused by the pandemic, others saw as an opportunity to use stolen identities to exploit programs and receive benefits to which they were not entitled. The consequences of these fraud schemes are both stolen relief funds and stolen identities.

Identity fraud is a crime that can result in at least three victims: the person whose identity is used to steal benefits, the person whose benefits are stolen, and the American taxpayer. Despite the magnitude of individuals impacted by this crime during the pandemic and the significant toll it takes on victims to clean up their personal credit scores, address tax consequences, and in some cases prove their eligibility for rightful benefits, many federal and state benefits agencies struggle to help victims resolve these complicated issues. Further, at the federal level there is no central entity responsible for holistically aiding and supporting victims throughout the redress process.

The PRAC's June 2022 report, [Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs](#), emphasized the need for government information-sharing and data matching to strengthen fraud prevention on the front end to reduce instances of identity fraud. Following the report issuance, the PRAC engaged MITRE, a not-for-profit federally funded research and development center, to conduct an independent study on the elements necessary for the development of a whole-of-government approach to identity fraud redress. As detailed in the attached report, MITRE interviewed victims of identity fraud who described the federal government's decentralized redress process as "burdensome, messy, confusing, isolating, and frustrating." As such, MITRE proposes development of a one-stop, claimant-centric redress model that enables victims to easily report identity fraud and receive support throughout the redress process. Such a model would require agencies to assist in a comprehensive manner while reducing the burden on the victims to resolve the issue themselves.

This report and the PRAC's June 2022 report provide specific actions the federal government could take to reduce identity fraud and establish a whole-of-government victim redress approach:

- Conduct data matching to verify identity and eligibility for government programs;
- Identify opportunities to rely on additional methods of identification and adjust fraud controls once a gap has been identified to help prevent similar fraud in the future;
- Establish interagency data sharing agreements consistent with applicable laws and regulations;
- Establish common practices and definitions across agencies through a National Identity Fraud Task Force to provide a consistent redress experience for victims; and
- Make multiple service channels available to victims of identity theft (e.g., in-person, telephone, online, and email) where legally permissible.

The PRAC will continue to work with Executive Branch officials and Congress to reduce identity fraud and improve victim redress processes in federal programs.



Michael E. Horowitz  
Chair, Pandemic Response Accountability Committee  
Inspector General, U.S. Department of Justice



# Identity **Fraud** Victim Redress Processes and Systems

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED # 23-22120.

**MITRE**

Center for Government  
Effectiveness and Modernization

Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843

## **NOTICE**

This (software/technical data) was produced for the U. S. Government under Contract Number TIRNO-99-D-00005, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data—General, Alt. II, III and IV (DEC 2007) [Reference 27.409(a)].

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

**© 2023 The MITRE Corporation.**

# Executive Summary

Victims of identity fraud interviewed for this report have called the current redress process, “burdensome, messy, confusing, isolating, and frustrating.”<sup>1</sup> According to the Pandemic Response Accountability Committee (PRAC), “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.”<sup>2</sup> Furthermore, the majority of the government employees interviewed for this assessment have expressed the need for standardization of policies,<sup>3</sup> articulated their need for better data sharing across government,<sup>4</sup> and requested better technology to create a seamless process.<sup>5</sup>

Discovering that you are a victim of identity theft is a traumatizing experience according to individuals interviewed for this report. When asked what adjectives individuals would use to describe the redress experience from the victim’s perspective, a national victim’s advocate stated, “I don’t have a single word to describe it, but [victims] feel very much that they’re not treated like a crime victim. The onus is on them to demonstrate their innocence and jump through all these hoops.”<sup>6</sup> This person went on to say, “we have a fundamentally different process for victims of identity crimes, and we make them feel like the criminal and we make them feel lost and alone, [as if] it’s totally up to them to resolve this issue and they have no support.”<sup>7</sup> Victims of identity theft, advocacy groups, and government officials interviewed for this study are asking for a true one-stop shop process with dedicated funding, where victims can conduct the federal redress process from grievance submission to resolution through one central application.

This report provides the strategic and tactical design elements necessary for this reimagined process by first framing federal redress as a single enterprise, then using inputs from interviews with victims of identity fraud, advocacy groups, and federal and state benefits administrators to develop a set of guiding principles for the design elements (five from the victim’s perspective and five from the government administrator’s perspective). Those guiding principles informed the development of a one-stop shop business framework, and a processing platform with detailed capabilities that shows how stakeholders would engage with this new platform. Though this report is a conceptual design of a strategic operating model, the report identifies three short-term, three mid-term, and three long-term considerations for the federal enterprise to consider as it moves from the proposed concept to implementation.

---

<sup>1</sup> National Victim’s Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>2</sup> Council of the Inspectors General on Integrity and Efficiency. Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs. By Pandemic Response Accountability Committee. Washington, DC: PRAC, 2022.

<sup>3</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022.

<sup>4</sup> Senior State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

<sup>5</sup> State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

<sup>6</sup> National Victim’s Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>7</sup> Ibid.

The nine considerations are broken into the following three categories:

1. Short-term considerations:
  - i. Establishing common thresholds and processes across government in accordance with the Payment Integrity Information Act (PIIA)<sup>8</sup> – Office of Management and Budget (OMB)
  - ii. Establishing inter-agency data sharing agreements – OMB
  - iii. Establishing a *no wrong door* federal policy that allows victims to report identity fraud to any federal agency using the full suite of service channels available across the federal enterprise, where permitted by law. – OMB
2. Mid-term considerations:
  - i. Conduct a macro-economic benefit-cost analysis to determine the return on investment of implementation. – OMB
  - ii. Develop a whole-of-government redress governance model. – OMB
  - iii. Run communications campaigns to inform the public of the existence of a new federal redress process. – Federal Trade Commission (FTC)
3. Long-term considerations:
  - i. Apply the Federal Integrated Business Framework (FIBF) to identify the granular requirements of this type of integration. – General Services Administration (GSA)
  - ii. Develop a federal fusion center for investigations. – OMB
  - iii. Congressional action required for implementation. – U.S. Congress

Incorporating these nine considerations into the identity fraud redress process would help alleviate the “burdensome, messy, confusing, isolating, and frustrating”<sup>9</sup> nature of the current decentralized federal redress process. The intent of this report is to provide key observations and insights that will transition the current federal redress process to a claimant-centric redress model founded on the principles of due process, which reduces the burdens on the victims of identity theft, empowers federal agencies to assist victims, and places the claimant at the center of all business decisions affecting operations across the federal identity theft redress space.

---

<sup>8</sup> Council of the Inspectors General on Integrity and Efficiency. *Guidance for Payment Integrity Information Act Compliance Reviews*. Washington, DC: Council of the Inspectors General on Integrity and Efficiency, 2021. <https://www.ignet.gov>.

<sup>9</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1-1</b>
1.1	Purpose and Overview of the Report .....	1-2
1.2	Scope.....	1-3
1.3	Key Definitions.....	1-4
1.4	Areas of Consideration .....	1-5
<b>2</b>	<b>Defining the Problem .....</b>	<b>2-1</b>
2.1	The Victim’s Perspective: Burden on The Claimant .....	2-2
2.1.1	How Does a Victim Seek ID Fraud Redress at the Federal Level? .....	2-5
2.2	The State and Federal Perspective .....	2-9
2.2.1	Frustrations with the Adjudication Process for Identity Theft Redress .....	2-10
2.2.2	Fixing Pay and Chase.....	2-12
<b>3</b>	<b>Guiding Principles for A Path Forward.....</b>	<b>3-1</b>
<b>4</b>	<b>The Design Elements of a New Redress Process.....</b>	<b>4-1</b>
4.1	One-Stop Shop Business Framework .....	4-1
4.2	Lifecycle Phases.....	4-3
4.3	One-Stop Federal Redress Platform.....	4-7
4.4	Redress Process Capability Needs .....	4-9
4.5	Past Implementations of One-Stop Platforms Across Government.....	4-13
4.5.1	State Government Implementation .....	4-13
4.5.2	Federal Government Implementation .....	4-13
4.6	The Benefits of Utilizing a Common Process Platform.....	4-14
4.6.1	Leveraging Best Practices.....	4-14
4.6.2	Capturing Economies of Scale.....	4-15
4.6.3	Shortening Claim Resolution Timeframes.....	4-15
4.6.4	Alleviating Common Victim Frustrations.....	4-16
4.6.5	Alleviating Common Government Employee Frustrations .....	4-17
4.6.6	Meeting the Intent of the Current Administration’s PMA and Executive Order (EO) 14058 .....	4-17
4.7	Use Cases .....	4-18
<b>5</b>	<b>Key Considerations .....</b>	<b>5-1</b>
5.1	Short-Term Considerations.....	5-1
5.1.1	Establish Common Thresholds and Processes .....	5-1
5.1.2	Establish Inter-Agency Agreements on Data Sharing .....	5-3
5.1.3	Make All Service Channels Available .....	5-3

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843**

5.2	Mid-Term Considerations.....	5-3
5.2.1	Conduct a Macro Economic Benefit-cost Analysis .....	5-3
5.2.2	Develop a Whole-of-Government Redress Governance Model .....	5-4
5.2.3	Run Communication Campaigns .....	5-5
5.3	Long-Term Considerations .....	5-6
5.3.1	Apply the Federal Integrated Business Framework (FIBF) .....	5-6
5.3.2	Fusion Center for Investigations .....	5-7
5.3.3	Congressional Action .....	5-7
<b>Appendix A</b>	<b>Acronyms .....</b>	<b>A-1</b>
<b>Appendix B</b>	<b>Methodology.....</b>	<b>B-3</b>
<b>Appendix C</b>	<b>Use Cases .....</b>	<b>C-1</b>
C.1	Initial Contact With Agency .....	C-1
C.2	Trauma Care Support .....	C-4
C.3	Request Federal Fraud Fusion Center Investigation .....	C-7



## List of Figures

Figure 2-2. Defining the Problem from a Victim's Perspective.....	2-5
Figure 3-1 Identity Fraud Redress Guiding Principles: An Enterprise Perspective .....	3-1
Figure 3-2 Guiding Principles: The Victim's Perspective.....	3-3
Figure 3-3 Guiding Principles: The Government's Perspective.....	3-4
Figure 4-1 One-Stop Shop Business Framework.....	4-2
Figure 4-2 Federal Redress Lifecycle Phases .....	4-6
Figure 4-3 Applicant Population Along the Redress Lifecycle .....	4-7
Figure 4-4 One-Stop Federal Redress Platform.....	4-8
Figure 4-5 Distribution of Capability Needs by Stakeholder .....	4-10
Figure 4-6 The Impacts of Automation and Using a Common Business Platform in Michigan .....	4-16
Figure B-1 Evaluation Methodology .....	B-3

## List of Tables

Table 1-1 Areas of Consideration for Victim Redress Processes and Systems .....	1-5
Table 2-1 Demographic Characteristics of Victims of Identity Theft and the U.S. Residential Population Age 16 or Older, 2018 .....	2-4
Table 3-1 Identity Fraud Victim Redress - Overall Needs by Cohort .....	3-4
Table 4-1 Potential Capability Needs with Description .....	4-10
Table C-1. Typical Flow of Events for Initial Contact with Agency.....	C-2
Table C-2. Typical Flow of Events for Trauma Care Support .....	C-5
Table C-3. Typical Flow of Events for Request Federal Fraud Fusion Center Investigation.....	C-8

# 1 Introduction

On March 11, 2020, the World Health Organization (WHO) declared that the spread of a novel coronavirus disease called SARS-CoV-2 (COVID-19) met the criteria for declaring a global pandemic. Around the same time, the U.S. Centers for Disease Control and Prevention (CDC) reported 60 cases of COVID-19 across 12 U.S. States.<sup>10</sup> In short order, the President of the United States declared a nationwide emergency that unlocked billions of dollars in federal funding to contain and combat the disease. The U.S. government focused the early days of the pandemic on virus containment, but that focus quickly broadened to the adverse economic realities associated with newly enforced pandemic restrictions.

The onset of COVID-19 left millions of Americans unemployed overwhelming state employment benefits systems. According to news reports in May 2020, “over 33 million Americans filed for initial jobless claims as a result of the coronavirus pandemic.”<sup>11</sup> An employee of a state unemployment office interviewed for this report when discussing the volume of claims their office was processing at the time said, “if another pandemic happens, I will retire because I can’t go through that again. We were working 16- to 17-hour days for about seven months. Even on Sundays we were having meetings. It was terrible. I don’t want to ever have to go through that again.”<sup>12</sup>

*“[During the pandemic] we were working 16- to 17-hour days for about seven months. Even on Sundays we were having meetings. It was terrible. I don’t want to ever have to go through that again.”<sup>13</sup> – Senior State Unemployment Office Employee*

---

For the purpose of this analysis – and consistent with previous MITRE research into benefits delivery – this report defines a benefit program as an intervention intended to “build equity, opportunity, and resilience for people by providing income or other resources to reduce poverty and inequality, support investments in human capital, and help insure against shocks and various risks” such as loss of income from disability or age, economic crisis, natural disaster and climate change.<sup>14</sup> Generally, governments provide benefits in three areas: “social assistance (noncontributory benefits and social services), social insurance (contribution-based benefits), and labor (both contributory and noncontributory benefits, as well as employment services).”<sup>15 16</sup>

---

<sup>10</sup> Centers for Disease Control and Prevention. "CDC Museum COVID-19 Timeline." CDC. Last modified August 16, 2022. <https://www.cdc.gov/museum/timeline/covid19.html> (accessed November 18, 2022)

<sup>11</sup> NBC News. "Over 76,000 Dead as 33 Million File for Unemployment in U.S." NBC News. Last modified May 8, 2020. <https://www.nbcnews.com/health/health-news/live-blog/2020-05-07-coronavirus-news-n1201801> (accessed November 18, 2022)

<sup>12</sup> Senior State Unemployment Official. Videoconference interview by the author. McLean, VA. November 8, 2022.

<sup>13</sup> Ibid.

<sup>14</sup> K. Lindert, T. G. Karippacheril, I. R. Caillava, and K. N. Chávez, eds., *Sourcebook on the Foundations of Social Protection Delivery Systems*, Washington, DC: World Bank, 2020. doi:10.1596/978-1-4648-1577-5. License: Creative Commons Attribution CC BY 3.0 IGO at 1.

<sup>15</sup> Ibid.

<sup>16</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.

According to the U.S. Government Accountability Office (GAO), problems such as the bureaucratic redundancies associated with benefit claims at the state and federal level, and limited logistical resources to process claims, led to bottlenecks in the delivery capacity of many benefit programs during the pandemic.<sup>17</sup>

The Washington Post reported that, “In the face of an unprecedented crisis, federal officials consistently chose haste over precision, dispatching aid with uncharacteristic speed to save the economy — even at the risk of costly mistakes.”<sup>18</sup>

The consequence of these actions was widespread identity fraud and theft that in turn pillaged unemployment insurance coffers across the country. Though the exact scope of this theft is unknown, according to press reports, “a top watchdog for the Labor Department estimated there could have been “at least” \$163 billion in unemployment-related “overpayments,” a projection that includes wrongly paid sums as well as “significant” benefits obtained by malicious actors.”<sup>19</sup> The largescale fraud is substantial, but it is critical to recognize the loss and impact suffered by victims of identity fraud and the challenges they face to restore their financial security and remedy losses through the vast and complex bureaucratic process available to them.

As detailed in section 4 of this report, this assessment defines a claimant-centric approach as one where all federal redress interactions with claimants are founded on the principles of due process while reducing the burdens on the victims of identity theft, placing the claimant at the center of all business decisions affecting operations across the federal space. A claimant-centric culture will enhance customer focus and reinforce trust between the public and the federal government. It will also empower government officials to address a victim’s concerns and process their application for redress efficiently.

This report begins with a focus on the victims’ perspectives, then addresses the federal adjudication process by understanding the limitations of current redress processes within certain federal benefits delivery agencies. Ultimately this assessment will provide an overview of the guiding principles of a redesigned federal identity theft redress process, as well as the strategic and tactical alternatives for implementation of a reimagined whole-of-government redress model.

## 1.1 Purpose and Overview of the Report

The objective of this report is to identify the necessary design elements for a federal identity theft and identity fraud redress processes related to government benefits programs. The Pandemic Response Accountability Committee (PRAC), a committee within the Council of the Inspectors General on Integrity and Efficiency (CIGIE) tasked by Congress to promote transparency and conduct oversight of the pandemic response,<sup>20</sup> contracted with The MITRE Corporation

---

<sup>17</sup> U.S. Government Accountability Office. *Lessons Learned When a Pandemic Led to Rapidly Rising Unemployment Claims*. Washington, DC: GAO, 2022. Accessed June 19, 2023. <https://www.gao.gov/blog/lessons-learned-when-a-pandemic-led-rapidly-rising-unemployment-claims>.

<sup>18</sup> Room, Tony, and Yeganeh Torbati. “A Magnet for Rip-off Artists’: Fraud Siphoned Billions from Pandemic Unemployment Benefits.” The Washington Post (Washington, DC), May 15, 2022., <https://www.washingtonpost.com/us-policy/2022/05/15/unemployment-pandemic-fraud-identity-theft/> (accessed November 18, 2022)

<sup>19</sup> Ibid.

<sup>20</sup> The PRAC’s oversight of the pandemic response is related to The Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020, The Families First Coronavirus Response Act, Paycheck Protection Program and Health Care Enhancement Act, The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), the Continued Assistance Act, and the American Rescue Plan Act (ARPA).

(MITRE) to conduct this work. As a federally funded research and development center operator authorized by Federal Acquisition Regulation 35.017, MITRE provides unbiased and conflict-free advice, guidance, and technical subject matter expertise to government sponsors.

To develop this report, MITRE's analysis included evaluation of federal and state approaches, policies, technology, and processes for implementing identity fraud redress programs. The analysis was conducted through review of federal and state documentation and as well as interviews with federal and state stakeholders. This analysis seeks to provide the PRAC the necessary strategic and tactical considerations to implement a whole-of-nation U.S. model for victim redress from federal benefit programs. This report will identify the guiding principles of this redesign, as well as provide cogent articulation of a new federal identity theft redress business process.

## 1.2 Scope

This report identifies strategic and tactical design elements needed to redesign the *federal* redress policies, systems, and systems across federal agencies. Though researchers for this report interviewed State officials to understand their perspective of the federal process, the intent was to glean their perspective on how a federal system can best address the States concerns. This report relied on inputs from an academic environmental scan that The MITRE Corporation conducted on behalf of the PRAC. The environmental scan consisted of two phases: 1) a review of academic literature and government publications; and 2) interviews with key stakeholders representing victim advocacy organizations, administrators and independent inspectors of government benefit programs, and victims of identity theft and fraud. Furthermore, the environmental scan focused on six Federal Agencies, notably the Social Security Administration (SSA), the Small Business Administration (SBA), the Federal Trade Commission (FTC), the Department of Veteran's Affairs (VA), the Department of Labor, and the Internal Revenue Service (IRS). The literature review examined the current perspective of identity fraud and provides context for what the federal government has done in the past and where future research should focus.

This report identifies strategic and tactical design elements needed to redesign the *federal* redress policies, systems, and systems across federal agencies. Though researchers for this report interviewed State officials to understand their perspective of the federal process, the intent was to glean their perspective on how a federal system can best address the States concerns. This report relied on inputs from an academic environmental scan that The MITRE Corporation conducted on behalf of the PRAC. The environmental scan consisted of two phases: 1) a review of academic literature and government publications; and 2) interviews with key stakeholders representing victim advocacy organizations, administrators and independent inspectors of government benefit programs, and victims of identity theft and fraud. Furthermore, the environmental scan focused on six Federal Agencies, notably the Social Security Administration (SSA), the Small Business Administration (SBA), the Federal Trade Commission (FTC), the Department of Veteran's Affairs (VA), the Department of Labor, and the Internal Revenue Service (IRS). The literature review examined the current perspective of identity fraud and provides context for what the federal government has done in the past and where future research should focus.

MITRE and the PRAC identified 33 interviewees from various U.S. federal and state government organizations, advocacy groups, and international organizations (e.g., Services

Australia). MITRE defined an evaluative framework of analysis to guide their research and interview approach. The three categories, advocacy groups, federal and state agencies and bridging opportunities provide perspectives related to the user experience, redress program capacity and applicable technologies to facilitate redress respectively.

The PRAC published an announcement on their website announcing the study. The PRAC sent an introductory email to prospective interviewees along with a calendar of available interview dates and a sample of interview questions. The mechanics of the interviews included one member facilitating the discussion and the other member taking notes. MITRE recorded the interviews and the duration ranged from 45-60 minutes in length. Individual team members analyzed and summarized interviews for insights related to each redress perspective.

The focus of this report being on the federal redress systems and process, there is little mention of fraud prevention requirements beyond ensuring that victims of identity fraud are protected from further victimization. As outline in section 2.2.2 of this report, changing the “pay and chase” mindset and instituting fraud prevention mechanism in tandem with a new redress process will help further this goal. In an effort to rely on evidence-based design, this report uses the framework of a one-stop shop redress which requires victims to initiate a claim to seek redress. There are very few examples of a no-stop shop process where governments would proactively start the redress process without having received a complaint from their constituents. Where those no-stop shop models exist there is not enough evidence to support a proper comparison of the benefits of one model over the other.

## **1.3 Key Definitions**

### **Identity Theft**

Identity theft is the criminal act of stealing personal, private, or financial information with the intent of using it to assume another person’s identity.

### **Identity Fraud**

The use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person.

### **Redress**

To remedy or set right for a wrong or grievance.

### **Improper Payments**

Government Accountability Office (GAO) Report Number GAO-02-749, August 2002, defines improper payments as payments that should not have been made or were made for incorrect amounts. Specifically, this includes inadvertent erroneous payments, such as duplicate payments, and incorrectly calculated payments (which may include underpayments or overpayments).<sup>21</sup>

### **Eligibility Fraud**

---

<sup>21</sup> Government Accountability Office. “Improper Payments.” <https://www.gao.gov/improper-payments> (accessed November 22, 2022)

Intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right as it relates to providing false or misleading information or omissions regarding eligibility for federal/state benefit programs; failure to notify the agency of any significant changes that might affect eligibility or eligibility level, or misuse of public assistance funds or benefits.<sup>22</sup>

## Federal Assistance/Benefit Programs

An intervention intended to “build equity, opportunity, and resilience for people by providing income or other resources to reduce poverty and inequality, support investments in human capital, and help insure against shocks and various risks.”<sup>23</sup>

## 1.4 Areas of Consideration

Table 1-1, represents a high-level summary of the different areas for consideration elucidated in this report. Starting at the conceptual level with a strategic perspective that encompasses guiding principles, a conceptual framework, and a business process, then moving to a tactical perspective that includes an operational platform, and nine next steps to move toward implementation.

**Table 1-1 Areas of Consideration for Victim Redress Processes and Systems**

Category	Proposed Consideration
<p><b>Guiding Principles - Detailed in Section 3 of This Report.</b></p>	<p><b>Victim’s Perspective:</b></p> <ul style="list-style-type: none"> <li>➤ Create a one-stop-shop.</li> <li>➤ Provide trauma-informed assistance.</li> <li>➤ Establish the principles of due process and fairness throughout the engagement.</li> <li>➤ Establish equity, inclusivity, accessibility, and security by offering appropriate service channels.</li> <li>➤ Keep the victim informed throughout the process.</li> </ul> <p><b>Administrator’s Perspective:</b></p> <ul style="list-style-type: none"> <li>➤ Establish redress programs and policies that define clear authorities.</li> <li>➤ Dedicate funding for redress programs.</li> <li>➤ Facilitate data sharing across government silos.</li> <li>➤ Standardize redress thresholds, policies, and language across government.</li> <li>➤ Minimize impacts to current operations and budgets.</li> </ul>

<sup>22</sup> U.S. Citizenship and Immigration. “Chapter 2 - Overview of Fraud and Willful Misrepresentation.” <https://www.uscis.gov/policy-manual/volume-8-part-j-chapter-2> (accessed November 4, 2022)

<sup>23</sup> K. Lindert, T. G. Karippacheril, I. R. Caillava, and K. N. Chávez, eds., *Sourcebook on the Foundations of Social Protection Delivery Systems*, Washington, DC: World Bank, 2020. doi:10.1596/978-1-4648-1577-5. License: Creative Commons Attribution CC BY 3.0 IGO at 1.

Category	Proposed Consideration
<b>Conceptual Framework – Detailed in Section 3 of This Report</b>	This report views the future design of the federal identity fraud redress process as one enterprise that encompasses four key stages of engagement, as identified in Figure 3-1 below.
<b>Business Process Framework – Detailed in Section 4.1 of This Report</b>	The proposed one-stop shop model for federal identity theft redress would serve as an integrated benefit delivery system. Specifically, a one-stop shop is “a single point of contact “where governments can collect data for one or more services through a single, integrated digital form” and deliver services and information from different entities. <sup>24</sup> The one-stop shop allows each benefits delivery agency to continue to work within their lane of authority and exercise their expertise in their benefits space. Although an applicant may go to one central location to apply for redress if, for example, a criminal fraudulently used their identity at IRS and SBA, each agency would be able to conduct its own investigation into the matter and provide periodic updates to the applicant while sharing data with other benefits delivery agencies participating in this shared framework. This ensures the applicant only goes to one location to seek relief, while other benefits delivery agencies can flag that applicant’s personally identifiable information (PII) to ensure they apply extra scrutiny to any request for benefits given the pattern of fraud.
<b>Operational Platform – Detailed in Section 4.3 of This Report.</b>	Within the context of the enterprise perspective of the redress process defined in Figure 3-1 below, this platform would serve as the line of visibility between the applicant and all participating benefits delivery agencies. Furthermore, this platform comprises the core design elements that satisfy the capabilities of this new system. Figure 4-4 depicts the one-stop federal redress platform and includes a capability list applicable to all the stakeholders who interact with these processes.
<b>Next Steps – Detailed in Section 5 of This Report</b>	Though this report is a conceptual design of a strategic operating model, the report identifies 3 short-term, 3 mid-term, and 3 long-term considerations for the federal enterprise to consider as it moves from the proposed concept to implementation. Section 5 provides further details of key considerations for implementation.

<sup>24</sup> Becker, Jorg, Marek Kowalkiewicz, Willem Martens, and Hendrik Scholta. "From One-Stop Shop to No-Stop Shop: An E Government Stage Model." *Government Information Quarterly* 36, no. 1 (January 2019): 11-26. [https:// www.sciencedirect.com/science/article/pii/S0740624X17304239](https://www.sciencedirect.com/science/article/pii/S0740624X17304239) (accessed March 24, 2023)



## 2 Defining the Problem

Increasing trust in government through effective management of government institutions is a critical component of the current administration's Presidential Management Agenda (PMA). In the PMA, the administration states that the manner in which "the public interacts with Government programs and benefits influences their level of trust in Government as an institution [...] delivering results and being accountable for [public sector] actions will steadily rebuild trust between the public and their government."<sup>25</sup> Seeking redress from the federal government should be a seamless process where the claimant (the victim of a crime) can request an investigation into their claim and, if the facts support their claim, be brought to a pre-injury condition; this is what this report generally refers to as identity fraud redress. In accordance with the aspirations of the PMA, delivering results to these victims is at the core of rebuilding trust in government institutions and reinforcing legitimacy in public institutions.

*"[A redress process] needs to be conceived on the front end of any type of program. I don't think it is an overstatement to say that [our agency] hadn't thought of a redress process [until] it was midstream, and millions of applications had already hit, and the hotlines were exploding. ... If you operate from the mindset of not putting [a process in place] on the front side, and not contemplating that there's going to be a loss or theft then I think you're going to find yourself behind the Eightball"<sup>26</sup> – Federal Deputy Inspector General*

---

The reality of the current redress process is divorced from this vision of an effective government. Victims of identity fraud interviewed for this report have called the current redress process, "burdensome, messy, confusing, isolating, and frustrating."<sup>27</sup> Furthermore, most of the government employees interviewed for this assessment have expressed the need for standardization of policies,<sup>28</sup> articulated their need for better data sharing across government,<sup>29</sup> and requested better technology to create a seamless process.<sup>30</sup> A senior state unemployment official when discussing customer service levels to claimants stated that, "everyone that I worked with really wanted to help [claimants]. [Applicants] were in dire straits and [state employees] were really looking for solutions. They were trying more than one avenue. They [would] make connections with people in other departments to try to help the claimants get benefits. We saw extraordinary levels of service ... [yet] we can always make better use of technology [to support our staff]."<sup>31</sup> Speaking to the need for better policies at the federal level, a federal deputy inspector general stated that a redress process, "needs to be conceived on the front end of any type of program. I don't think it is an overstatement to say that [our agency] hadn't thought of a redress process [until] it was midstream, and millions of applications had already hit, and the

---

<sup>25</sup> The President's Management Council. *The Biden-Harris Management Agenda Vision Toward an Equitable, Effective, and Accountable Government that Delivers Results for All*. Washington, DC: Office of Management and Budget, 2021.

<sup>26</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022.

<sup>27</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>28</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022.

<sup>29</sup> Senior State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

<sup>30</sup> State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

<sup>31</sup> Senior State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

hotlines were exploding ... If you operate from the mindset of not putting [a process in place] on the front side, and not contemplating that there's going to be a loss or theft then I think you're going to find yourself behind the Eightball.”<sup>32</sup>

Ultimately, the current federal process for redress places the burden on the victims of identity theft to navigate a complex bureaucracy. Current federal policies require the victim to engage with each benefits-delivery agency in a process that most victims interviewed for this report characterize as “frustrating and burdensome.”<sup>33</sup> Continuing the status quo discounts the trauma associated with being a victim of identity theft.

## 2.1 The Victim's Perspective: Burden on The Claimant

Discovering that you are a victim of identity theft is a traumatizing experience according to individuals interviewed for this report.<sup>34</sup> When asked what adjectives individuals would use to describe the federal identity theft redress process from the victim's perspective a national victim's advocacy stated, “I don't have a single word to describe it, but [victims] feel very much that they're not treated like a crime victim. The onus is on them to demonstrate their innocence and jump through all these hoops. Can you imagine if we did that to victims of sexual assault or to family members of homicide victims?”<sup>35</sup> This person went on to say that, “we have a fundamentally different process for victims of identity crimes and we make *them* feel like the criminal and we make them feel lost and alone, [as if] it's totally up to them to resolve this issue and they have no support.”<sup>36</sup>

*“I don't have a single word to describe it, but [victims] feel very much that they're not treated like a crime victim. The onus is on them to demonstrate their innocence and jump through all these hoops. Can you imagine if we did that to victims of sexual assault or to family members of homicide victims? We have a fundamentally different process for victims of identity crimes, and we make them feel like the criminal and we make them feel lost and alone, [as if] it's totally up to them to resolve this issue and they have no support.”<sup>37</sup> – National Victim's Advocate*

---

The victims of identity fraud seeking redress from the federal government have multiple processes and procedures to navigate to submit claims for redress, assuming the agency has one. This places a burden on the victims to navigate the different federal bureaucracies.

*“I do not see any evidence that any one particular group is broadly targeted or falls victim more often than any other, however there are cohorts of people who have attributes that are similar. They're not your standard demographics, it's about how you engage in the outside world, with few exceptions. Now, the differently abled, (e.g., the blind, deaf, or hard of*

---

<sup>32</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022.

<sup>33</sup> Victim of Identity Theft. Videoconference interview by the author. McLean, VA. October 31, 2022.

<sup>34</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.

<sup>37</sup> Ibid.

*hearing) [will have] a lot of common vulnerabilities ... just because of those abilities ... I am vulnerable to all of these crimes and scams, so are you, again it's about how we engage [with] the outside world and making sure we setup our programs to address [those heightened vulnerabilities].”<sup>38</sup>*  
– National Victim’s Advocate

---

Besides being a general burden for the American public, the current identity fraud redress process also exposes a question of equity and accessibility for individuals with limited means or disabilities. While speaking to demographic vulnerabilities associated with identity theft, one national victim’s advocate said, “I do not see any evidence that any one particular group is broadly targeted or falls victim more often than any other, however there are cohorts of people who have attributes that are similar. They're not your standard demographics, it's about how you engage in the outside world, with few exceptions. Now, the differently abled, (e.g., the blind, deaf, or hard of hearing) [will have] a lot of common vulnerabilities ... just because of those abilities.” This advocate went on to say, “I am vulnerable to all of these crimes and scams, so are you, again it’s about how we engage [with] the outside world and making sure we setup our programs to address [those heightened vulnerabilities].”<sup>39</sup>

To validate these claims, we reviewed data from the Department of Justice’s (DOJ) Office of Justice Programs. The Bureau of Justice Statistics (BJS) published data explaining the makeup of victims of identity theft in 2018. **Error! Reference source not found.** (please see **Error! Reference source not found.**) shows that targets of identity theft are proportional to the demographic makeup of that population.<sup>40</sup> Furthermore, the report states that, “half of all victims of identity theft (51%) were in households with incomes of \$75,000 or more.”<sup>41</sup>

*“Victims of personal information misuse, [which includes unauthorized use of personal information for fraudulent purposes such as getting a government benefit] were more likely to experience severe emotional distress than [other victims].”<sup>42</sup>* – Dr. Erika Harrell, DOJ

---

---

<sup>38</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>39</sup> Ibid

<sup>40</sup> Harrell, Erika, Ph.D. Victims of Identity Theft, 2018. Research report no. NCJ 256085. Washington, DC: U.S. Department of Justice, April 2021.

<sup>41</sup> Ibid.

<sup>42</sup> Ibid.

**Table 2-1 Demographic Characteristics of Victims of Identity Theft and the U.S. Residential Population Age 16 or Older, 2018<sup>43</sup>**

-	Victims of Identity Theft			U.S. Residential Population	
Demographic Characteristics	Number of Victims	Percent of US Residential Population Age 16 or Older <sup>a</sup>	Percent of All Victims	Number of Persons Age 16 or Older	Percent of Persons Age 16 or Older
Total	23,183,020	9%	100%	258,175,200	100%
<b>Sex</b>					
Male*	11,219,660	9%	48.4%	125,188,140	48.5%
Female	11,963,360 †	9%	51.6% †	132,987,070	51.5%
<b>Race/Ethnicity</b>					
White <sup>b*</sup>	16,560,830	10.1%	71.4%	163,585,560	63.4%
Black <sup>b</sup>	2,100,740 †	6.8% †	9.1% †	30,846,330	11.9%
Hispanic	2,719,120 †	6.4% †	11.7% †	42,553,730	16.5%
Asian <sup>b</sup>	1,192,880 †	7.8% †	5.1% †	15,277,670	5.9%
Other <sup>b,c</sup>	609,440 †	10.3%	2.6% †	5,911,910	2.3%
<b>Age</b>					
16 - 17	99,310 †	1.2% †	0.4% †	7,979,760	3.1%
18 - 24	1,759,310 †	5.9% †	7.6% †	29,916,270	11.6%
25 - 34	4,410,270 †	9.8% †	19% †	44,892,670	17.4%
35 - 49*	6,772,500	11%	29.2%	61,627,990	23.9%
50 - 64	6,478,060	10.3% ‡	27.9%	62,994,100	24.4%
65 or older	3,663,570 †	7.2% †	15.8% †	50,764,410	19.7%
<b>Household income</b>					
\$24,999 or less	2,847,190 †	6% †	12.3% †	47,499,520	18.4%
\$25,000 - \$49,999	4,323,590 †	6.5% †	18.6% †	66,365,670	25.7%
\$50,000 - \$74,999	4,211,840 †	8.8% †	18.2% †	47,790,700	18.5%
\$75,000 or more*	11,800,400	12.2%	50.9%	96,519,310	37.4%

**Note:** Details may not sum to totals due to rounding. Estimates are based on the most recent incident of identity theft. Missing data for household income were imputed. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 4 in the source paper for standard errors.

\*Comparison group.

† Difference with comparison group is significant at the 95% confidence level.

‡ Difference with comparison group is significant at the 90% confidence level.

<sup>a</sup>Estimates are based on the number of persons in each category. For example, the percentage for males is the number of male victims of identity theft divided by the total number of males age 16 or older multiplied by 100.

<sup>b</sup>Excludes persons of Hispanic origin (e.g., “white” refers to non-Hispanic whites and “black” refers to non-Hispanic blacks).

<sup>43</sup> Ibid.

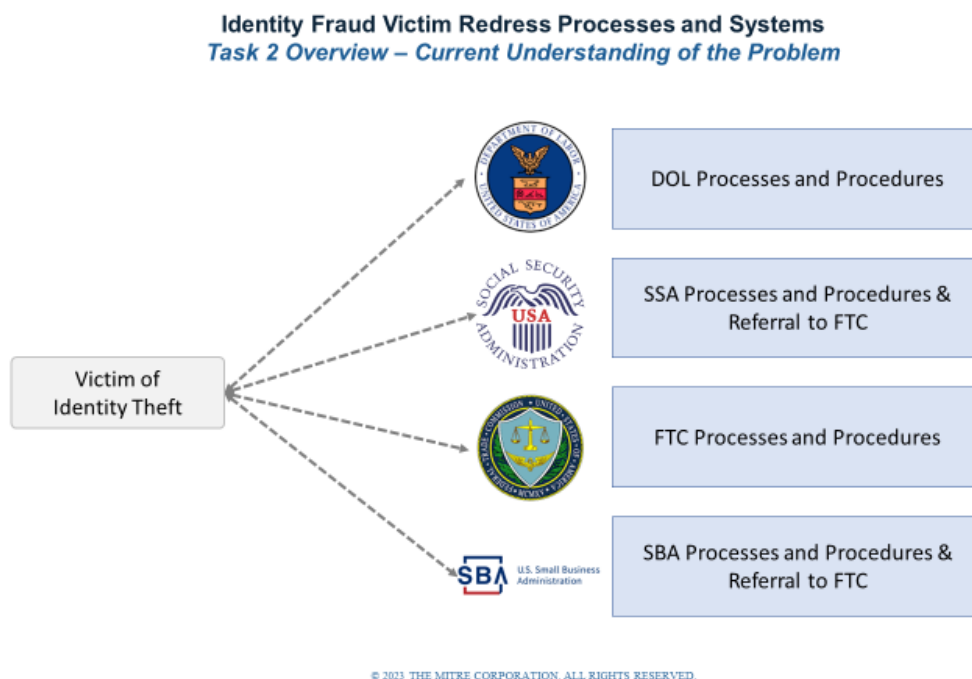
<sup>c</sup>Includes Native Hawaiians, Other Pacific Islanders, American Indians, Alaska Natives, and persons of two or more races.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

This report further highlights that “victims of personal information misuse, [which includes unauthorized use of personal information for fraudulent purposes such as getting a government benefit] were more likely to experience severe emotional distress than [other victims].”<sup>44</sup>

## 2.1.1 How Does a Victim Seek ID Fraud Redress at the Federal Level?

For the purposes of this report, we have developed a use case of an individual who had their identity stolen and used for fraudulent purposes. As identified in Figure 2-2, in this example, a criminal used the victim’s social security number (SSN) to apply for federal benefits such as the Paycheck Protection Program (PPP) loan through SBA. The criminal using this person’s SSN also applied for unemployment benefits under the Pandemic Emergency Unemployment Compensation Programs (PEUC). This use case will focus on 3 critical categories that relate to the claimant’s perspective: awareness, available service channels, and ease of communication.



**Figure 2-1. Defining the Problem from a Victim's Perspective**

### 2.1.1.1 Awareness

In this scenario the victim of identity theft would have to proactively engage with each federal agency where they think criminals may have used their identity leading to numerous potential phone calls to disparate agencies who each have their own rules around the redress process. This brings up two questions related to awareness:

1. When does a victim first realize that criminals have fraudulently used their identity?

<sup>44</sup> Ibid.

## 2. How does a victim learn about remedy available to them through the federal government?

### **2.1.1.1.1 When and How Do Individuals Learn they are Victims of Identity Theft?**

According to a senior state unemployment official, in some cases victims aren't aware until they get a "benefits card for unemployment benefits and didn't ask for it."<sup>45</sup> This would only occur if the "fraudster went in, filed the claim, and didn't change the address for whatever reason."<sup>46</sup> This official went on to say, "then we get calls from employers asking why [a current employee] is getting unemployment benefits."<sup>47</sup> In this case this official acknowledged that unless the fraudulent actor makes a mistake, the citizen won't know their identity was stolen until they get their tax filings at the end of the year.<sup>48</sup>

Victim notification needs to be part of any eventual solution, whether that requires a reimagining of how the American public tracks its benefit programs, or a focus on the use of technology to send push notifications to the American public anytime a person accesses a benefit program.

### **2.1.1.1.2 How do Victims Learn About Remedy Options Through the Federal Government?**

One of the concerns consistently articulated by victims and government officials interviewed for this assessment, is that individuals don't know where to start when they have their identity stolen. One senior state official stated, "It gets very frustrating very quickly [...] and I'm not the most sophisticated person, but obviously I was a professional [senior state official] for years and know how to do analysis. I could just imagine my brother [who is] a blue-collar worker going through this. He'd be calling me [asking] what [...] am I supposed to do here?"<sup>49</sup> Another national victim's advocate stated that there "is the need for one place for people to start [the redress process] without exception and not [multiple places]. You need one central place for people to start and we can argue about everything in the middle."<sup>50</sup>

*"[There] is the need for one place for people to start [the redress process] without exception and not [multiple places]. You need one central place for people to start and we can argue about everything in the middle."<sup>51</sup> –  
National Victim's Advocate*

---

A previous PRAC report identifies this concern by stating the following:

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

---

<sup>45</sup> Senior State Unemployment Official. Videoconference interview by the author. McLean, VA. November 8, 2022.

<sup>46</sup> Ibid.

<sup>47</sup> Ibid.

<sup>48</sup> Ibid.

<sup>49</sup> Victim of Identity Theft. Videoconference interview by the author. McLean, VA. October 31, 2022.

<sup>50</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>51</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.



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.<sup>52</sup>

### 2.1.1.2 Available Service Channels

Once the victim in our use case is aware of the fraud, they will attempt to contact each of the organizations where the criminal fraudulently used their identity, and other organizations where they think their identity may have been used (e.g., credit reporting agencies and banks). When asked which service channels they would prefer to use when contacting government, respondents to a Pew Research survey stated:

1. Telephonic communications – preferred by 40-percent of respondents<sup>53</sup>
2. Website visits – preferred by 29-percent of Americans<sup>54</sup>
3. In person visits – preferred by 20-percent of Americans<sup>55</sup>
4. Email communication – preferred by 11-percent of Americans<sup>56</sup>
5. Smart phone apps – which are not currently widely available to the public.

*“You go [to] that identitytheft.gov, and maybe it's because I'm not as tech savvy, [but] I didn't see a chat [function where] I could chat with somebody. Could I call somebody? Can I e-mail someone? It's just like, here's an automated system ... You're not talking to a human being, you're talking to AI [...], and AI is great in certain circumstances, but when I'm a victim and I'm frustrated and I'm feeling like, oh, my God, my credit is ruined, I can never unfreeze my credit if I ever apply for a loan again ... to not be able to talk to a human being is frustrating.”<sup>57</sup> – Victim of Identity Theft*

---

Each federal agency has different ways that claimants can interact with them. The varying available service channels provide our victim a very different experience with each organization. Some agencies do not provide victims the ability to communicate with a live person. During conversations with a national victim’s advocate group, one senior official said, “a lot of people prefer the phone [because] they want to talk to a real live human being, and a lot of times it's not just the advice that we give them, it's how it's presented. And because this is a traumatic experience, they need that trauma informed care.”<sup>58</sup> When speaking directly to a victim of identity theft they told us, “You go [to] that identitytheft.gov and maybe it's because I'm not as tech savvy, [but] I didn't see a chat [function where] I could chat with somebody. Could I call somebody? Can I e-mail someone? It's just like, here's an automated system ... You're not

---

<sup>52</sup> Executive Council of the Inspectors General on Integrity and Efficiency. Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs. By Pandemic Response Accountability Committee. Washington, DC: PRAC, 2022.

<sup>53</sup> Pew Research Center. "How Americans Get in Touch with Government." Pew Research Center. Last modified May 24, 2004. Accessed November 18, 2022. <https://www.pewresearch.org/internet/2004/05/24/how-americans-get-in-touch-with-government/>.

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.

<sup>56</sup> Ibid.

<sup>57</sup> Victim of Identity Theft. Videoconference interview by the author. McLean, VA. October 31, 2022.

<sup>58</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

talking to a human being, you're talking to [artificial intelligence] (AI) [...], and AI is great in certain circumstances, but when I'm a victim and I'm frustrated and I'm feeling like, oh, my God, my credit is ruined, I can never unfreeze my credit if I ever apply for a loan again ... to not be able to talk to a human being is frustrating.”

#### **2.1.1.2.1 Equity and Accessibility**

Having multiple service channels available to victims of identity theft also helps with the concern of equity and accessibility for individuals with disabilities, and individuals who do not speak English as their primary language or have limited English proficiency. A senior SSA official when addressing this issue stated, “because many of our customers cannot use online services, they visit our offices, or they call us. Those are the folks [for whom] English is not their first language, they have severe mental impairments, they’re elderly, there are just any number of barriers that our customers face. That's why we put so much effort into authenticating the customer when they are in front of us when we have them with us, and we do a lot, we spend a lot of time with them explaining because our programs are so complex.”<sup>59</sup>

The number of service channels proposed in any government-wide redress model needs to ensure victims of identity theft have access to the appropriate avenues that consider the traumatic nature of the harm inflicted on them (e.g., trauma informed advisors). Furthermore, the redress process should ensure ease of accessibility to individuals with disabilities, and other demographics that have aggravating conditions (e.g., individuals with limited English proficiency, or a person under supervised care). Ultimately these service channels need to be compliant with federal civil rights statutes and executive orders (EO) to ensure agencies are providing their services in a manner that is accessible for individuals with disabilities and those who have limited English proficiency. EO 13985, titled “*Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*,” explicitly requires that federal agencies also ensure their programs reach underserved communities.<sup>60</sup>

#### **2.1.1.3 Ease of Communication**

After identifying the proper service channel, our use case victim will submit a claim for redress at the different federal agencies that oversee the benefit programs that were fraudulently accessed. Some federal agencies such as SSA, SBA, and the IRS will refer victims seeking redress in identity theft cases to a U.S. Federal Trade Commission (FTC) operated website called [identitytheft.gov](https://identitytheft.gov). Victims of identity theft, when talking about [identitytheft.gov](https://identitytheft.gov), have stated, “it was very frustrating to get emails and not be able to talk to a human being. Then to go into that system and basically be told things I already know [wasn’t] helpful to me. I went in, did the checklist, and by the time I got to the end of it, it's like [...] You’re not telling me anything I don't know. It was just [saying] freeze your credit, monitor your credit, and that's about it.”<sup>61</sup> A national victim’s advocate stated that, “time is of the essence when they're trying to begin this process, and they can't do it for days, weeks, sometimes months, if [the FTC] keeps pointing them at different jurisdictions.”<sup>62</sup> The inability to get regular updates on an application status or

---

<sup>59</sup> Senior Social Security Administration Official. Videoconference interview by the author. McLean, VA. November 15, 2022.

<sup>60</sup> Exec. Order No. 13985, 86 Fed. Reg. 7009 (Jan. 25, 2021). <https://www.federalregister.gov/d/2021-01753/page-7009> (accessed December 7, 2022)

<sup>61</sup> Victim of Identity Theft. Videoconference interview by the author. McLean, VA. October 31, 2022.

<sup>62</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.



speak to a person that can provide situational clarity into the process is a frustration that current victims of identity fraud face.

## 2.2 The State and Federal Perspective

All the state and federal government officials interviewed for this report had one common trait. They were all dedicated public servants who work tirelessly to support the citizens of their respective jurisdictions. One state employee agreed with the statement that “on average most federal and state employees want to do right by the citizens they serve.”<sup>63</sup> Employees at the different federal benefits delivery agencies included in this scan take identity theft and identity fraud seriously. For the most part, these organizations have invested heavily in technology to authenticate individuals applying for benefits, to include facial recognition technology, two-step authentication, and in some cases the use of algorithms and filters to identify suspicious behavior. This is on top of the manual processes instituted to authenticate applicants, which include mandatory in-person visits to offices, and manual reviews of application patterns to identify application inconsistencies. These measures focus on prevention of fraud. One senior IRS official said, “The majority of [our work] is identity theft filtering ... We do this in a multi-prong approach. The first piece is we have models and filters in two different systems that act differently, and this is our return review program and our dependent database. We also utilize a manual fraud detection where we're looking for link analysis [through] various patterns and trends that might not be picked up by our filters. So, we've got that manual component and we apply resources to those analytics.”<sup>64</sup> When asked if this particular component works primarily on the prevention side versus the redress side of identity fraud, this official said, “yes that is correct ... We started introducing pre refund filters and the creation of the Taxpayer Protection program that allowed an interaction with the taxpayer very early in the process before the refund is paid so that taxpayer interacting with the IRS will confirm who they say they are, and then the IRS will just release that refund.”<sup>65</sup>

*“We've had a lot of success in in our fraud prevention activities. [...] We have been able to prevent millions, 10s of millions of dollars in benefits from being paid because we've caught them before the claim was actually paid. [...] We are successful in preventing fraud, but in terms of the identity theft redress, I don't know of any sort of KPIs that we have.”<sup>66</sup> Senior SSA Official*

---

One senior SSA employee said, “We've had a lot of success in in our fraud prevention activities. We have a number of things that we're doing [such as] fraud prevention units that look at potentially fraudulent cases. We have a workload support unit that looks at anomalous claims and we've been able to identify what could be potentially fraudulent activity. [...] We've been able to prevent payment of benefits by identifying those anomalous claims. So that's one indication for us if we can catch them before benefits are paid. We have these cooperative

---

<sup>63</sup> Senior State Unemployment Official. Videoconference interview by the author. Mclean, VA. November 8, 2022.

<sup>64</sup> Senior Internal Revenue Service Official. Videoconference interview by the author. McLean, VA. November 07, 2022.

<sup>65</sup> Ibid.

<sup>66</sup> Senior Social Security Administration Official. Videoconference interview by the author. McLean, VA. November 15, 2022.

disability investigation units, which are these units that we have representing all of our states and territories. It's a collaborative effort with operations, OIG, and our state Disability Determination Services. What they do is they look at potentially fraudulent claims that are filed and they investigate those claims. [Those claims are] referred to these units and we have been able to prevent millions, 10s of millions, of dollars in benefits from being paid because we've caught them before the claim was actually paid. So those are some indicators that we use to show that we are successful in preventing fraud, but in terms of the identity theft redress, I don't know of any sort of key performance indicators (KPI) that we have.”<sup>67</sup>

These preventive measures against identity fraud have proven to be effective at mitigating fraudulent benefits payments and reducing the caseload for identity fraud redress. Inevitably there will be instances where preventive measures will fail, and agencies will pay fraudulent benefits claims. This was apparent during the COVID-19 pandemic where, according to press reports, “a top watchdog for the Labor Department estimated there could have been “at least” \$163 billion in unemployment-related “overpayments,” a projection that includes wrongly paid sums as well as “significant” benefits obtained by malicious actors.”<sup>68</sup>

The federal and state employee perspective identified in this report centers on two main themes:

1. Frustration with the current identity fraud redress process, which includes a need to:
  - a. Establish redress policies and establish clear authorities.
  - b. Standardize thresholds and policies across the government.
  - c. Dedicate funding for redress programs.
2. The need to fix the “pay and chase” mentality around benefits delivery.

## **2.2.1 Frustrations with the Adjudication Process for Identity Theft Redress**

Federal and state employees who assist victims navigate the federal identity theft redress process have expressed frustration with redress processes, or the lack thereof. Undoubtedly this cohort of stakeholders on average are dedicated to assisting their constituents within the bounds of their statutory and/or regulatory authority. During the COVID-19 pandemic these employees found themselves working long hours to assist victims navigate the federal process. An employee of a state unemployment office interviewed for this report when discussing the volume of claims their office was processing at the time said, “[during the pandemic] we were working 16- to 17-hour days for about seven months. Even on Sundays we were having meetings. It was terrible. I don’t want to ever have to go through that again.” The gaps in the current federal redress process, are not because of a lack of willingness to serve the victims of identity theft and fraud, rather we consistently heard state and federal employees are frustrated with the following three elements of the identity theft redress process:

1. The lack of established identity theft redress processes within certain institutions.

---

<sup>67</sup> Ibid.

<sup>68</sup> Romm, Tom, and Yeganeh Torbati. "A Magnet for Rip-off Artists': Fraud Siphoned Billions from Pandemic Unemployment Benefits." The Washington Post (Washington, DC), May 15, 2022. Accessed November 18, 2022, <https://www.washingtonpost.com/us-policy/2022/05/15/unemployment-pandemic-fraud-identity-theft/>.

2. The lack of standardization of thresholds and policies when those policies exist.
3. The need for dedicated funding for redress programs to ensure prioritization.

*“There needs to be dedicated funding for [a redress process] because that is how priorities are set. Whether it's at the Congressional level or [at the Executive level], it needs to be funded because that to me indicates it's a priority. But to ask agencies to take this on as an unfunded need, I think that's where you're going to have difficulty [implementing an effective redress process] ... [especially since across government] we're facing a historic staffing and attrition crisis in our agencies. I cannot keep my frontline employees and I know other agencies are in the same place. So, for this to be a priority within SSA, it really would have to be funded. It could not just be something that I could absorb.”<sup>69</sup> – Senior Social Security Administration Official*

---

### **2.2.1.1 Need to Establish Redress Policies and Establish Clear Authorities**

This report finds that only IRS, the VA and SBA of the six agencies of interest for this report have an existing identity theft and identity fraud redress process. The other three agencies neither have an existing policy, internal investigation processes, or provide an official remedy to victims of identity theft. All six agencies have invested heavily in identity theft and identity fraud prevention.

In one case, prior to the influx of identity fraud claims due to COVID-19, a federal agency did not have a redress policy in place until millions of applicants had submitted their claims.<sup>70</sup> Thankfully this agency had the ability to quickly establish a process for their constituents to seek redress. One federal deputy inspector general in an interview for this report identified that no matter the level of defenses in place some fraud will come through and you need to have a redress process in place to assist the victims of identity fraud.<sup>71</sup>

This sentiment was consistent across interviews with state and federal employees. One state employee speaking to the lack of policies that facilitate coordination between the states and the federal government stated, “it was a frustration, and back in 2009 I actually spoke at a forum in DC and [told them] you are so focused on agencies and the Beltway, you don't even realize what's happening out at the local level or at the state level. You've got to get your head outside [the Beltway]. [There needs to be a] focus on working with States because the money's coming to the State and then it's passing through to the locals. [I went on to tell them], if you're focused on the federal agencies and the District of Columbia (D.C.), you're missing 90% of the issue.”<sup>72</sup>

### **2.2.1.2 Standardization of Thresholds and Policies**

Where federal agencies have existing redress policies in place (for the purposes of this report these agencies are the SBA and the IRS), there is a lack of standardization of thresholds for what constitutes identity theft, and those agencies conceived existing redress policies within

---

<sup>69</sup> Senior Social Security Administration Official. Videoconference interview by the author. McLean, VA. November 15, 2022.

<sup>70</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022

<sup>71</sup> Ibid.

<sup>72</sup> Former Senior California State Official. Videoconference interview by the author. McLean, VA. October 31, 2022.

institutional silos. This ultimately means that the victim of identity fraud will consistently have a different experience as they seek redress from different federal agencies unless there is collaboration across silos to establish best practices through standardization of processes where permissible by statute and regulation.

One senior SSA official speaking to the concern of standardization stated that, “every agency has unique processes and would need information in order to verify identity theft. It's starting at a threshold matter. We are working [internally] with the agency on what qualifies as an identity theft event. [...] How are you going to vet this? Does there have to be a financial loss? What thresholds would you use?”<sup>73</sup>

### **2.2.1.3 Dedicated Funding for Redress Programs**

Having dedicated funding for a program initiative has a dual effect. It first ensures that you have the proper resources to address the problem (e.g., personnel and tools), and second it is a signaling mechanism to administrators that the program is essential. Dedicated funding also comes with specific KPIs. A senior SSA official interviewed for this report stated, “there needs to be dedicated funding for [a redress process] because that is how priorities are set. Whether it's at the Congressional level or [at the Executive level], it needs to be funded because that to me indicates it's a priority. But to ask agencies to take this on as an unfunded need, I think that's where you're going to have difficulty [implementing an effective redress process] ... [especially since across government] we're facing a historic staffing and attrition crisis in our agencies. I cannot keep my frontline employees and I know other agencies are in the same place. So, for this to be a priority within SSA, it really would have to be funded. It could not just be something that I could absorb.”

### **2.2.2 Fixing Pay and Chase**

The Washington Post reported that, “In the face of an unprecedented crisis, federal officials consistently chose haste over precision, dispatching aid with uncharacteristic speed to save the economy — even at the risk of costly mistakes.”<sup>74</sup> Though the exact scope of this theft is unknown, according to press reports, “a top watchdog for the Labor Department estimated there could have been ‘at least’ \$163 billion in unemployment-related ‘overpayments,’ a projection that includes wrongly paid sums as well as ‘significant’ benefits obtained by malicious actors.”<sup>75</sup> It is important to understand the economic reality Americans faced in the throes of this pandemic. According to news reports in May 2020, “over 33 million Americans filed for initial jobless claims as a result of the coronavirus pandemic, which routed some industries to Depression-era levels.”<sup>76</sup> Beyond the health emergency, COVID-19 had also engendered an economic crisis for the American people.

---

<sup>73</sup> Senior Social Security Administration Official. Videoconference interview by the author. McLean, VA. November 04, 2022.

<sup>74</sup> Romm, Tom, and Yeganeh Torbati. “A Magnet for Rip-off Artists’: Fraud Siphoned Billions from Pandemic Unemployment Benefits.” The Washington Post (Washington, DC), May 15, 2022. <https://www.washingtonpost.com/us-policy/2022/05/15/unemployment-pandemic-fraud-identity-theft/> (accessed November 18, 2022)

<sup>75</sup> Ibid.

<sup>76</sup> NBC News. “Over 76,000 Dead as 33 Million File for Unemployment in U.S.” NBC News. Last modified May 8, 2020, <https://www.nbcnews.com/health/health-news/live-blog/2020-05-07-coronavirus-news-n1201801> (accessed November 18, 2022)

Federal and state employees interviewed for this report sympathized with the economic reality at the time but stated that a situation where an agency pays the total amount allowable under statute and seeks reimbursement from a third party is ineffective because it is very difficult to collect on those funds; this situation is colloquially known as “pay and chase.” One federal deputy inspector general stated that prevention on the front end “will cut down the volume for redress on the backend [...] if you don’t have a process in place to verify eligibility in a meaningful way, this is what you see. I don’t believe the problem is redress. You can’t pay and chase.”<sup>77</sup>

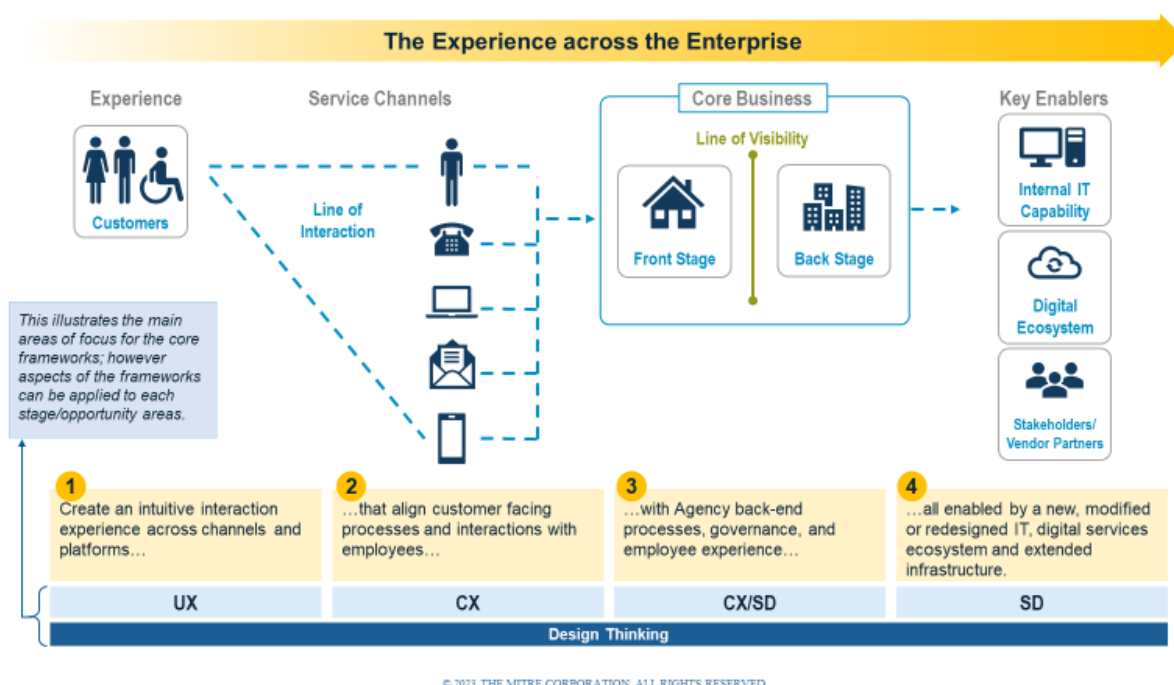
Research for this environment scan and the interviews with federal officials have led to one key observation that prevention and redress policies must be instituted in tandem with one another. It is difficult to separate these two processes because a lack of preventative measures will overwhelm any redress system in place.

---

<sup>77</sup> Federal Deputy Inspector General. Videoconference interview by the author. McLean, VA. November 11, 2022

### 3 Guiding Principles for A Path Forward

Prior to developing a detailed whole-of-government redress process and identifying the design elements required to support it, this report develops the precepts that place the claimant at the center of the federal redress process and empowers agencies to provide a remedy to the victims of identity fraud. These guiding principles should stay constant irrespective of changes in strategies, goals, or leadership. To this end, this report enumerates these guiding principles based on the interactions with victims of identity theft, government employees (both state and federal) who interface with these victims and have oversight over the redress process, and identity fraud victim's advocates groups.



**Figure 3-1 Identity Fraud Redress Guiding Principles: An Enterprise Perspective**

With the understanding that guiding principles set a standard for how an organization operates, this report starts by viewing the future design of the federal identity fraud redress process as one enterprise that encompasses four key stages of engagement, as identified in Figure 3-1:

1. Service channels that would serve as the line of interaction for the public, and account for the need for trauma-informed care, and accessibility as identified in Section 4.1 of this report.
2. The front stage of the core business, which in this case would be the central customer facing process. Here the public would have a common feel when engaging in the redress process across government.
3. The backstage of the core business where back-end interconnected systems and processes would operate by facilitating the investigation and adjudication process. A line of visibility separates this stage of the engagement from the front stage, which this report identifies in Section 4.3 as the one-stop redress platform. This will allow each benefits

delivery agency to continue to work within their lane of authority and exercise their expertise in their benefits space.

4. The key system enablers such as the IT capabilities and the digital ecosystem that supports data collection, transmission, storage, and security.

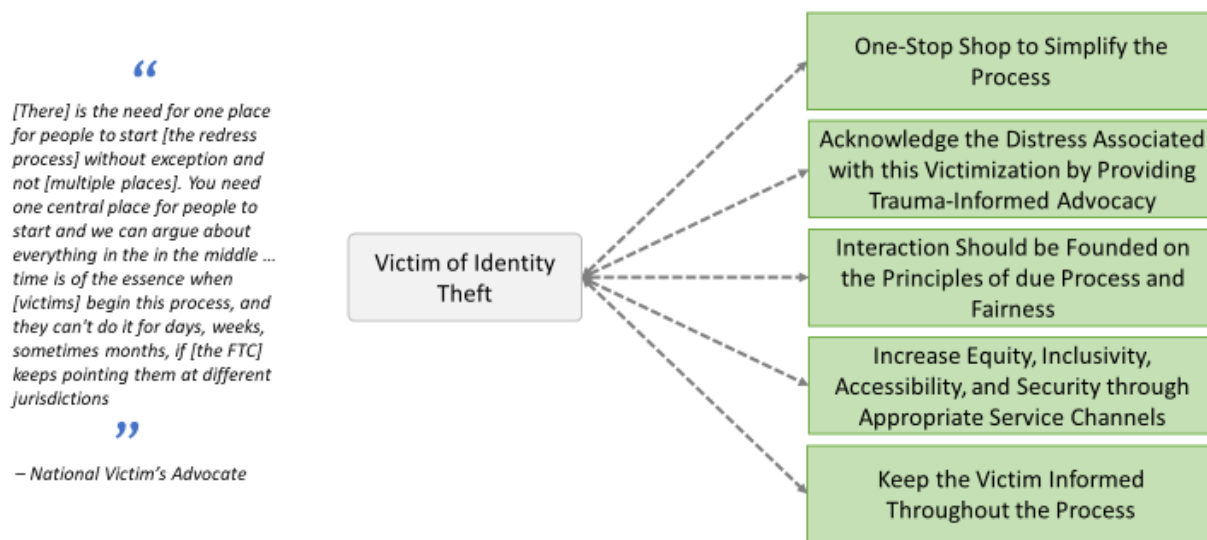
Each stage of the enterprise engages two central stakeholders:

1. The victims of identity fraud who are submitting a claim to seek redress, and
2. The government officials who process redress claims.

Figure 3-2 provides a graphical representation of the guiding principles associated with the victim's perspective. These guiding principles include:

1. The federal redress process should be viewed from an enterprise perspective where claims are processed via a one-stop shop to ease the burden on the victim.
2. The process should acknowledge the distress associated with being a victim of identity theft by providing trauma-informed care and advocacy.
3. Victim interactions with the federal redress enterprise should be founded on the principles of due process and fairness.
4. The federal redress process should increase equity, inclusivity, accessibility, and security through the appropriate service channels because identity theft cuts across all demographics, including individuals with limited English proficiency and individuals with disabilities.
5. Keep the victims of identity theft informed throughout the redress process.

**Identity Fraud Victim Redress Processes and Systems**  
*Summary of Guiding Principle: Claimant-Centric Approach to Empower Agencies*



© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

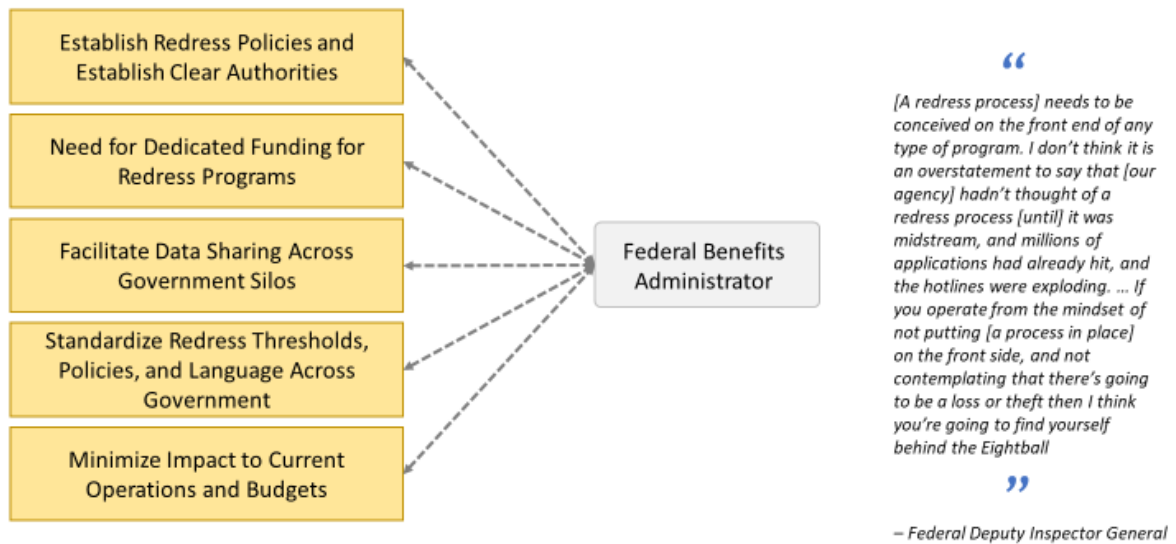
**Figure 3-2 Guiding Principles: The Victim's Perspective**

Figure 3-3 provides a graphical representation of the guiding principles associated with the federal benefits administrator's perspective. These guiding principles include:

1. Establish an identity fraud redress process with clear policies that delineate authorities and responsibilities.
2. Provide dedicated funding for redress programs.
3. Facilitate data sharing across government silos.
4. Standardize redress thresholds, policies, and language across government.
5. Minimize impacts on current operations and budgets.



**Identity Fraud Victim Redress Processes and Systems**  
*Summary of Guiding Principle: A Claimant-Centric Approach that Empowers Agencies*



© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

**Figure 3-3 Guiding Principles: The Government's Perspective**

These ten guiding principles, summarized in **Error! Reference source not found.**, have informed the design elements identified in Section 4 of this report.

**Table 3-1 Identity Fraud Victim Redress - Overall Needs by Cohort**

Needs	Victim Needs	State and Federal Needs
1	Create a one-stop-shop.	Establish redress programs and policies that define clear authorities.
2	Provide trauma-informed assistance.	Dedicate funding for redress programs.
3	Establish the principles of due process and fairness throughout the engagement.	Facilitate data sharing across government silos.
4	Establish equity, inclusivity, accessibility, and security by offering appropriate service channels.	Standardize redress thresholds, policies, and language across government.
5	Keep the victim informed throughout the process.	Minimize impacts to current operations and budgets.

## 4 The Design Elements of a New Redress Process

Addressing the problems identified in Section 2, while incorporating the themes from the guiding principles in Section 3, requires the federal government to adopt a digital transformation and embrace a streamlined one-stop shop claimant-centric approach. This will revolutionize the way victims of identity fraud interact with federal benefits-delivery agencies. The model provides claimants the ability to login into one central platform and have access to all the benefits delivery agencies participating in this framework, as opposed to having to seek redress from each individual agency.

This section will start by developing a business framework for the redesigned redress process, then define the lifecycle phases of this new framework. The report will then pivot to a detailed explanation of the design elements of the platform needed to make the business framework operational. Lastly this section will develop a hypothesis of analysis based on available authoritative research pertaining to integrated benefits delivery both in the US and overseas. This research takes a comparative view of why, and how, government institutions have integrated their benefits delivery system and is based on findings from organizations such as MITRE, the World Bank, Code for America, The Center for Budget and Policy Priorities (CBPP), and other peer-reviewed journal articles.

### 4.1 One-Stop Shop Business Framework

The proposed one-stop shop model for federal identity theft redress would serve as an integrated benefit delivery system. This report defines an integrated benefit system as “the mechanism by which the different government stakeholders in the benefits space interconnect systems, processes, and platforms to create a system that ensures the ease of service delivery by serving the public quickly, securely, and equitably.”<sup>78</sup> Specifically, a one-stop shop is “a single point of contact “where governments can collect data for one or more services through a single, integrated digital form” and deliver services and information from different entities.”<sup>79</sup> The one-stop shop is defined by the following features: integrated data collection without proactive or predictive benefits delivery.<sup>80</sup> It is a centralized platform for delivering e-government services.<sup>81</sup> In a one-stop shop, the interface, or front office, is designed such that the benefit seekers use one interface to request services from the various government departments.<sup>82</sup> The one-stop shop “requires that all public authorities are interconnected and that the [benefits seeker] is able to access public services at a single point even if these services are provided by different public authorities or private service providers.”<sup>83</sup> In sum, the centrality of the services should be

---

<sup>78</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.

<sup>79</sup> Becker, Jorg, Marek Kowalkiewicz, Willem Martens, and Hendrik Scholta. "From One-Stop Shop to No-Stop Shop: An E Government Stage Model." *Government Information Quarterly* 36, no. 1 (January 2019): 11-26. <https://www.sciencedirect.com/science/article/pii/S0740624X17304239> (accessed March 24, 2023)

<sup>80</sup> Ibid.

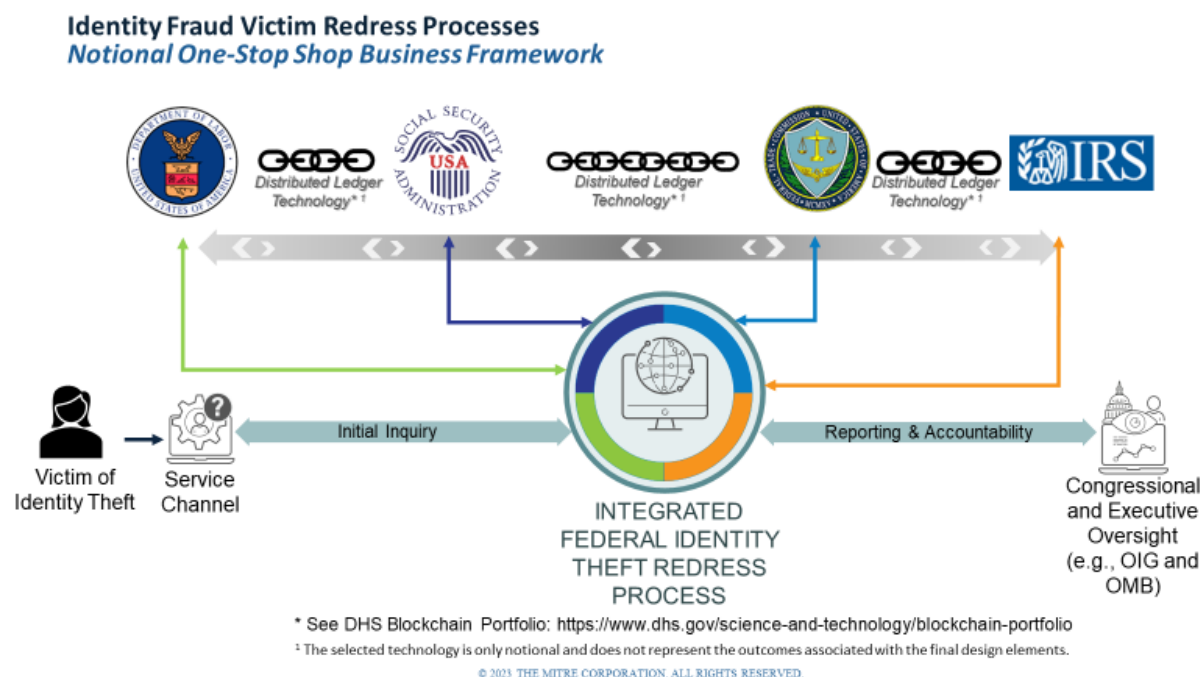
<sup>81</sup> Ibid.

<sup>82</sup> Ibid.

<sup>83</sup> Wimmer, Maria A. "A European Perspective Towards Online One-Stop Government: The eGOV Project." *Electronic Commerce Research and Applications* 1, no. 1 (Spring 2002): 92-103.

apparent to the applicant, since they have only one centralized location to request benefits that cut across government.”<sup>84</sup>

Notably the one-stop shop allows each benefits delivery agency to continue to work within their lane of authority and exercise their expertise in their benefits space. Although an applicant may go to one central location to apply for redress if, for example, a criminal fraudulently used their identity at IRS and SBA, each agency would be able to conduct its own investigation into the matter and provide periodic updates to the applicant while sharing data with other benefits delivery agencies participating in this shared framework. This ensures the applicant only goes to one location to seek relief, while other benefits delivery agencies can flag that applicant’s personally identifiable information (PII) to ensure they apply extra scrutiny to any request for benefits given the pattern of fraud.



**Figure 4-1 One-Stop Shop Business Framework**

The business process illustrated in Figure 4-1 serves as a basis for the one-stop federal redress platform outlined in Section 4.3 below. This new business process would allow an applicant to pick one of five service channels to submit a redress claim to all benefits delivery agencies who participate in the redress platform. Those service channels include:

1. In-person at local offices
2. Telephonic customer support
3. Online application and submission with secure data sharing

<https://www.sciencedirect.com/science/article/pii/S156742230200008X?viewFullText=true> (accessed March 9, 2023)

<sup>84</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843**

4. iOS and Android Applications
5. Mail

Once the claimant submits this application, the system would route information to the relevant agency where there is known fraudulent data and share the applicant's data across participating agencies (where it is not explicitly prohibited by statute) to prevent further fraud associated with the claimant's PII. The agencies would also be able to share data and request data from the applicant via the applicant's service channel of choice. Finally, this integrated platform would be able to aggregate reporting and accounting data for federal and congressional oversight. Though this high-level one-stop shop business framework outlines the general process, the one-stop federal redress platform outlined in Section 4.3 will provide further details.

## 4.2 Lifecycle Phases

For the purpose of this analysis – and consistent with previous MITRE research into benefits delivery – this report defines a benefit program as an “intervention intended to ‘build equity, opportunity, and resilience for people by providing income or other resources to reduce poverty and inequality, support investments in human capital, and help insure against shocks and various risks’ such as loss of income from disability or age, economic crisis, natural disaster and climate change.”<sup>85</sup> <sup>86</sup> To this end, seeking redress from the federal government is intrinsically a benefits seeking activity because an individual is attempting to mitigate a risk, and needs to actively request that the government investigate, adjudicate, and remedy the alleged wrong.

In 2020, the World Bank published a report titled *Sourcebook on the Foundation of Social Protection Delivery Systems*. The World Bank report is an assessment of benefits delivery systems through an international comparative analysis and identifies nine common phases of the benefits delivery process. In this study, we use the findings of the World Bank report to inform our description of the federal redress lifecycle. Seeking redress for the fraudulent use of one's identity requires a victim to submit an application that an institution needs to process as they would any other benefit determination.

Below, this analysis provides an in-depth description of the redress lifecycle phases.

1. **Outreach and Education:** This is a requirement to convey the existence of the redress process to the public. Benefits delivery agencies must educate the potential registrant of the availability of that program's benefit. Whether done proactively or passively, there is a requirement to communicate the availability of the redress processes to the public. Inputs for this business requirement include messages, communication tools, and active

---

<sup>85</sup> K. Lindert, T. G. Karippacheril, I. R. Caillava, and K. N. Chávez, eds., *Sourcebook on the Foundations of Social Protection Delivery Systems*, Washington, DC: World Bank, 2020. doi:10.1596/978-1-4648-1577-5. License: Creative Commons Attribution CC BY 3.0 IGO at 1.

<sup>86</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.

searches.<sup>87</sup> Outputs for this phase of the lifecycle include identifying the intended population groups and ensuring they understand the program.<sup>88</sup>

2. **Applicant Intake and Registration:** This is how individuals apply for assistance and engage with the redress programs. Intake is the process of gathering information, while registration is the process of recording and verifying that information.<sup>89</sup> Benefits agencies must intake applicant information or they cannot process claims. This is the phase where the five service channels described in section 4.1 will play a central role as the line of interaction for the public, and account for the need for trauma-informed care, inclusivity, and accessibility. The primary input for this requirement is people applying for benefits.<sup>90</sup> “The primary output for [this phase of the lifecycle] is having complete information on the applicant that is verified and validated for use as an input to the assessment of needs and conditions.”<sup>91</sup>
3. **Assessment of Needs and Conditions:** This requirement is part of the adjudication process. It constitutes the due diligence requirements of each program to validate the information provided during the application intake. Furthermore, it is consistent with the guiding principle of having a redress process that is founded on the principles of due process and fairness. This phase is also an initial assessment for the level of restitution that the applicant is due based on their specific conditions. The input for this requirement is complete, validated and verified information. The output produced is a completed profile of the applicant.<sup>92</sup>
4. **Eligibility and Enrollment:** With a completed profile of the registrant, the benefits agencies would then compare the registrant’s profile to the eligibility criteria derived by that program’s statutes or regulations to determine eligibility and make a decision on the applicant’s claim. The output of this requirement is a rules-based determination.<sup>93</sup> This fact-based determination could be anything from freezing the victim’s benefits to avoid any further damage, to referring the applicant’s case to the US Department of Justice.
5. **Determination of Benefits and Services:** Once the benefits agency has made a rules-based decision on the applicant’s eligibility they must decide how much restitution the victim should receive based on the facts of the claim.<sup>94</sup>
6. **Notification and Onboarding:** The benefits programs would then notify all parties to the claim of the eligibility decision and the determination of benefits. The agencies would also onboard that claimant by explaining the rules and conditions of their eligibility, and how they can better protect their identity and use their benefit.<sup>95</sup>

---

<sup>87</sup> K. Lindert, T. G. Karippacheril, I. R. Caillava, and K. N. Chávez, eds., *Sourcebook on the Foundations of Social Protection Delivery Systems*, Washington, DC: World Bank, 2020. doi:10.1596/978-1-4648-1577-5. License: Creative Commons Attribution CC BY 3.0 IGO.

<sup>88</sup> Ibid.

<sup>89</sup> Ibid.

<sup>90</sup> Ibid.

<sup>91</sup> Ibid.

<sup>92</sup> Ibid.

<sup>93</sup> Ibid.

<sup>94</sup> Ibid.

<sup>95</sup> Ibid.

7. **Provision of Benefits and Services:** Benefits agencies must ensure restitution is funded in accordance with the eligibility decision and the determination of benefits and services sent to the parties of the claim. Inputs for this phase of the process includes the applicant's account information (if a disbursement of funds is necessary). Output includes the payment of benefits to the claimant.
8. **Benefits Compliance, Updating, and Grievances:** Benefits agencies must be able to comply with statutory and regulatory stipulations of their programs that call for oversight. This includes maintaining a system of record for audits and oversight management. The benefits agencies must conduct beneficiary operations management to ensure the beneficiary's continuity of eligibility (e.g., the IRS Pin Program). Agencies can do this through periodic reassessments. Agencies must also ensure that applicants can file grievances and appeals through the management of some grievance redress mechanisms (GRM).<sup>96</sup>
9. **Exit Decision, Notification and Case Outcomes:** The agencies would notify beneficiaries who are no longer eligible, or who have been fully compensated for the benefit to which they are entitled, that they will be exiting the program. As a part of compliance efforts to the public overseers of benefits agencies, the benefits delivery agencies must capture and store metadata on the case outcomes and explain how the agency's financial intervention affected the cohort of interest.

Figure 4-2 provides an overview of the inputs and outputs of the lifecycle phases defined above, as well as a flow of how requirements depend on one another along the benefits delivery chain. Figure 4-3 provides a view of the registrant and applicant pool as they move along the benefits delivery chain up to the provision of benefits requirement. As this delivery chain progresses, through each step, the population shrinks.

---

<sup>96</sup> Ibid.

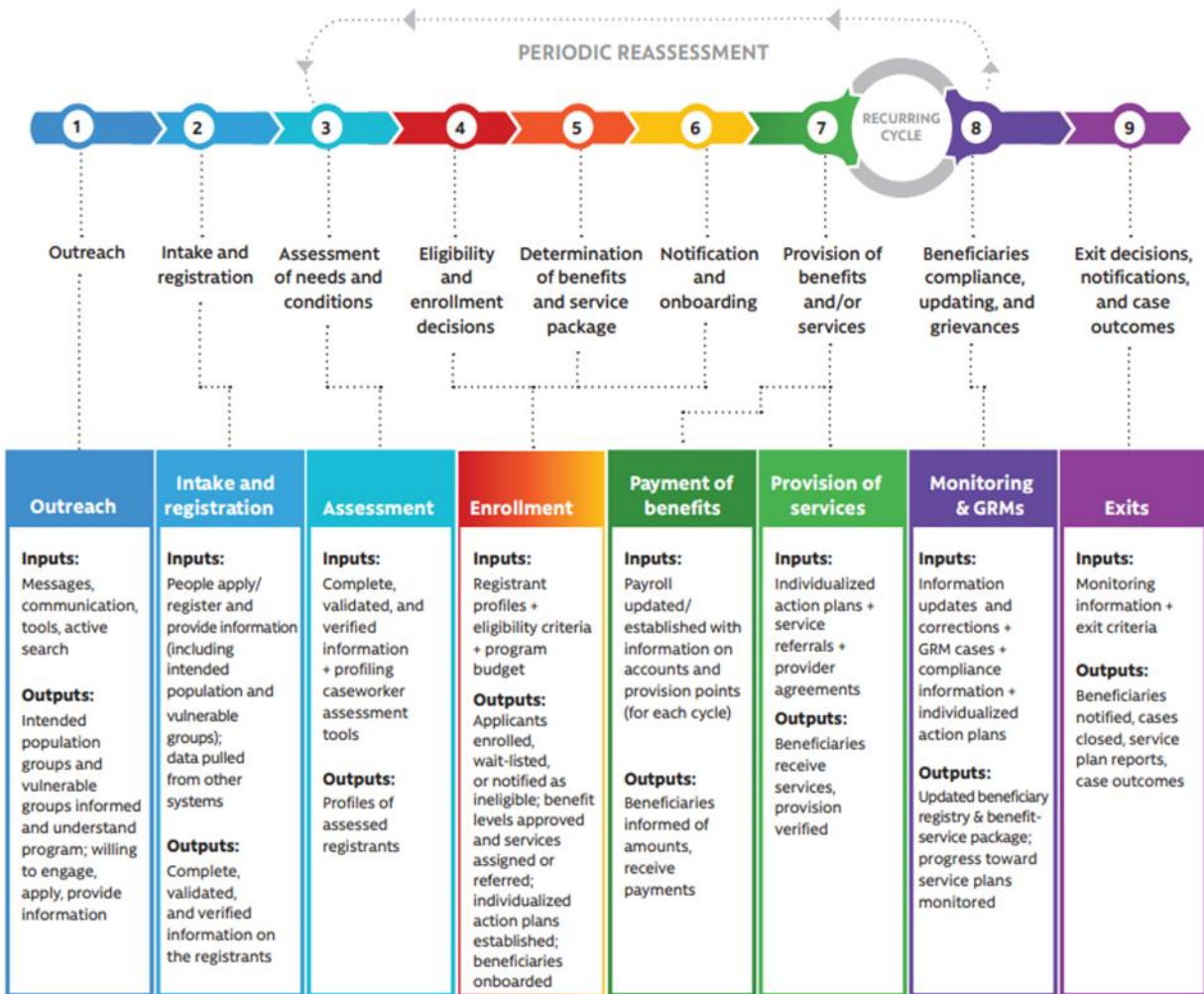


Figure 4-2 Federal Redress Lifecycle Phases<sup>97</sup>

<sup>97</sup> Ibid.



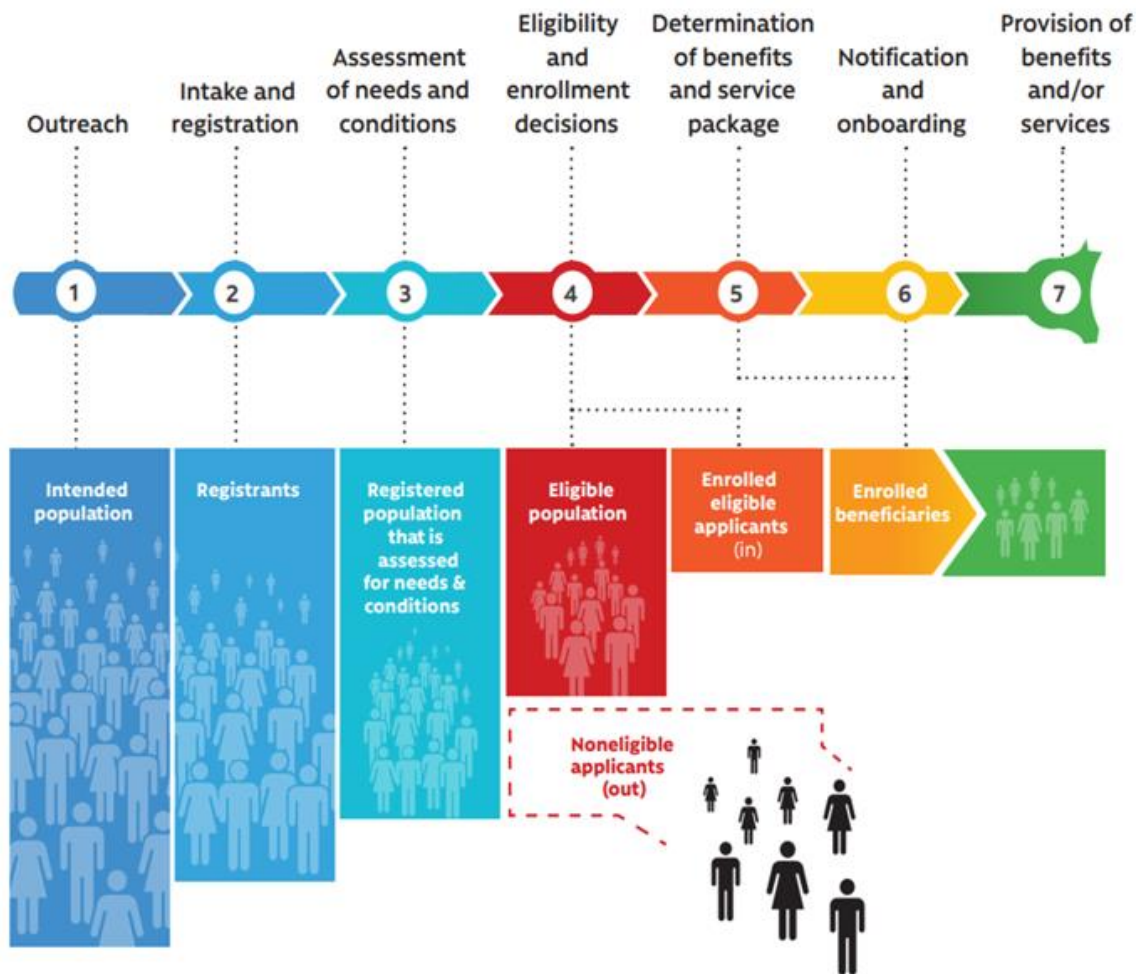


Figure 4-3 Applicant Population Along the Redress Lifecycle<sup>98</sup>

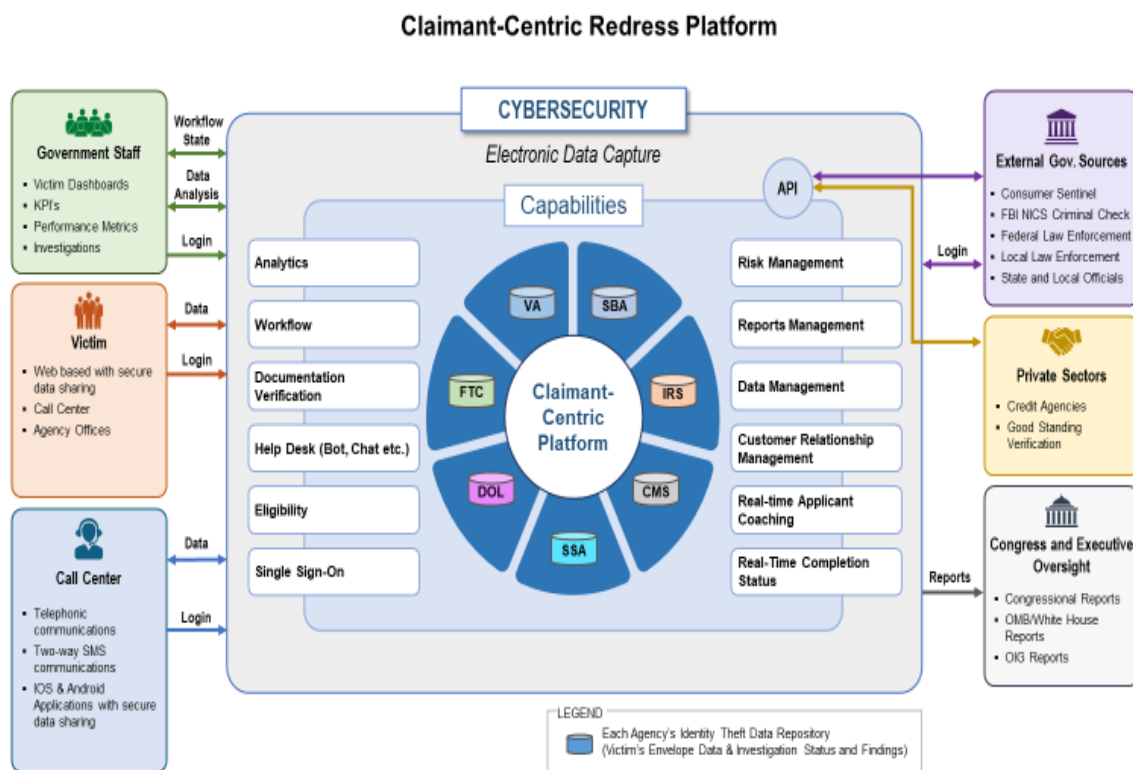
### 4.3 One-Stop Federal Redress Platform

The one-stop shop business process identified in Figure 4-1 informed the development of the one-stop federal redress platform below in Figure 4-4. Whereas the guiding principles elucidated in Section 3 provides high-level precepts for two key stakeholders (i.e., the victim and the government staff), this platform provides a detailed review of the many stakeholders who support and oversee the redress process. Within the context of the enterprise perspective of the redress process defined in Figure 3-1 above, this platform would serve as the line of visibility between the applicant and all participating benefits delivery agencies. Furthermore, this platform comprises the core design elements that satisfy the capabilities of this new system. Figure 4-4 depicts the one-stop federal redress platform and includes a capability list applicable to all the stakeholders who interact with these processes. There are six categories of stakeholders:

<sup>98</sup> Ibid.



1. **Government Staff:** These are the government officials who process the redress claims at the various participating agencies. This would require a workflow state, data analytics capabilities, and a secure login into the database.
2. **Claimant:** These are the individuals who seek redress for an incident of identity fraud.
3. **Call Center:** These are the individuals who receive calls through that service channel. Call centers can also process two-way short message service (SMS) communications, as well as Android and iOS application requests and questions.
4. **External Gov Sources:** These parties include Federal Agencies who manage the databases used for criminal investigations (e.g., FBI NICS and FTC Consumer Sentinel). This category of stakeholders also includes the state and local officials who manage programs that interact with the participating federal benefits delivery agencies.
5. **Private Sector Parties:** This includes the private sector partners who can serve as a pipeline for notification of fraud, as well as the organizations and databases federal employees use for good standing verification of the applicant.
6. **Congressional and Executive Oversight:** This includes congressional oversight committees, the Office of Management and Budget (OMB), and public auditors.



© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

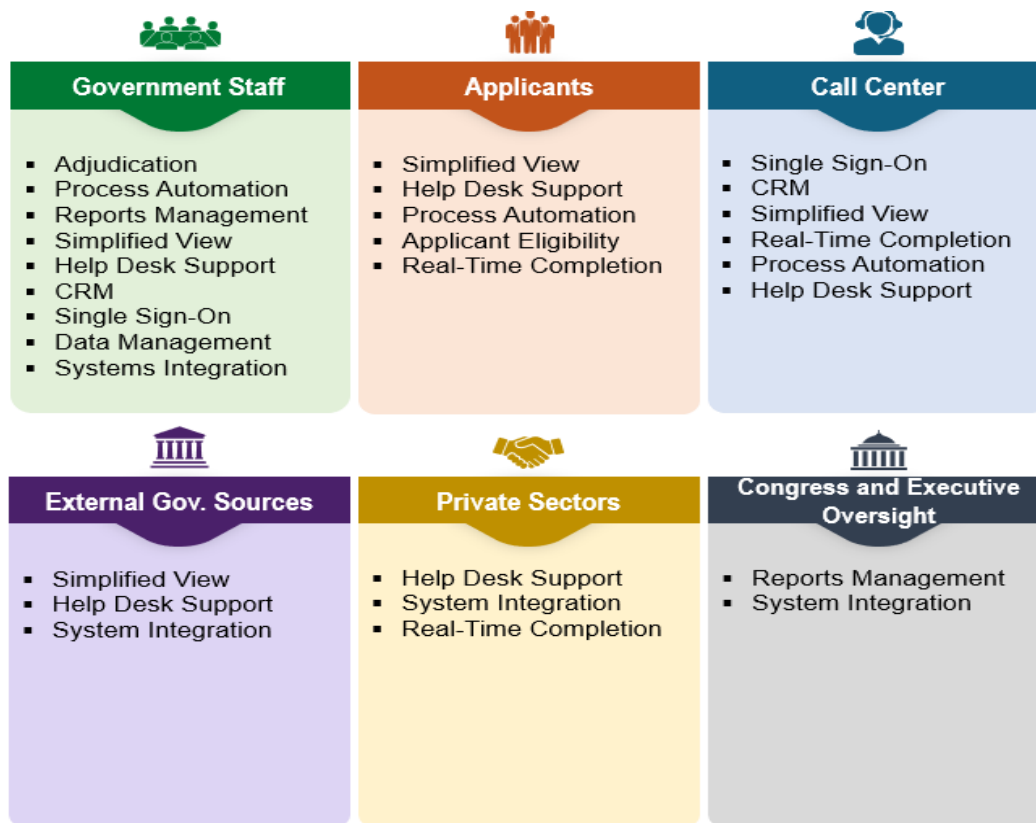
**Figure 4-4 One-Stop Federal Redress Platform**

## 4.4 Redress Process Capability Needs

The stakeholders listed in section 4.3 need the following proposed capabilities as part of the design elements of the new one-stop shop identity fraud redress process:

1. The ability to exchange applicant information in a digital format in real time.
2. The ability to securely authenticate and prescreen applicant data.
3. The ability for government employees to login once for access to systems and applications required to process the applicant's file.
4. The ability to readily access source data throughout the course of the claims investigation process to make an informed adjudication of the facts as presented by the applicant and the parties to the claim. This would support investigative efforts across federal agencies.
5. The ability to have a simplified view of the complete applicant file.
6. The ability to automate data capture and data processing.
7. The ability to integrate/interface with external systems via file transfer, webservice, or application programming interface (API).
8. The ability to integrate all reporting systems to provide canned and ad hoc reporting.
9. The ability for all parties to reach help desk support for all processes (technical and non-technical).
10. The ability for applicants to have a real-time completion status on the progression of their request.

Figure 4-5 below provides a distribution of these capability needs by stakeholder.



© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

**Figure 4-5 Distribution of Capability Needs by Stakeholder**

Table 4-1 provides a breakdown of capabilities by providing a detailed description of that capability.

**Table 4-1 Potential Capability Needs with Description**

Capability Title	Capability Description
Analytics	A system or capability that can retrieve data from the claimant-centric hub, combine and derive information from it to be used for review and analysis.
Cloud Platform	The service used to provide on-demand availability of computer system resources, including data storage and computing power, without direct active management by the user to house custom software, PaaS platforms and SaaS software systems.

Capability Title	Capability Description
Customer Relationship Management (CRM)	A tool, strategy, or process that helps business better organize, access, analyze and manage customer data.
Data Management	The practice of collecting, keeping, organizing, maintaining, and using data securely and efficiently.
Document Management	A system used to receive, track, and store documents.
Document - OCR Scanning	A technology used to distinguish printed or handwritten text characters inside digital images to enable the parsing into defined datapoints.
Documentation Verification	This tool will provide a “verify before validate” rule “verifying” that the documents submitted by the victims are complete and accurate before proceeding to the “validation” of the documents.
Eligibility	Eligibility automation tools are an initial step before the investigative process. Eligibility automation will enable claimants to verify they meet all the eligibility requirements for redress.

Capability Title	Capability Description
Risk Management	<p>This tool will identify claimants with complex situations that have a higher propensity for fraud and tag them as high risk; and those with a less complex situations and thus a lower propensity for fraud and tag them as low risk. This risk determination will assist in triaging applications for the government staff who investigate each case. Agencies will determine the risk assessment factors based on past indicators of fraud since bad actors may fraudulently apply for redress.</p>
Help Desk	<p>A service and associated tools to provide information and support to users.</p>
Real-Time Coaching	<p>This tool will guide the victims throughout each screen with a real-time clear user-friendly description of what they need to submit on the specific screen. Throughout each step, if the tool discovers some discrepancy, the claimant will be notified in real-time what is needed to correct the issue before moving to the next screen.</p>
Workflow	<p>A platform or tool to sequence administrative or other processes through which a piece of work passes from initiation to completion.</p>
Workflow – Data Integration	<p>A platform or tool, specific to data integration, to sequence, join, and parse data as the work using such data passes from initiation to completion.</p>

## 4.5 Past Implementations of One-Stop Platforms Across Government

Implementing the proposed one-stop federal redress platform necessitates a review of other integrated benefits delivery systems and one-stop style systems across the United States at the state and federal government levels.

### 4.5.1 State Government Implementation

In December 2021 MITRE published a report on integrated benefits delivery. The report, titled “Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe,” revealed that U.S. States have successfully integrated their delivery of disparate federal benefits, including the Supplemental Nutrition Assistance Program (SNAP) operated by the U.S. Department of Agriculture (USDA), Medicaid, and the Low-Income Home Energy Assistance Program (LIHEAP) operated by the U.S. Department of Health and Human Services (HHS).<sup>99</sup> The report further noted that the CBPP and Code for America have partnered with other public benefits corporations and states to run a project called “The Integrated Benefits Initiative.”<sup>100</sup> The pilot is focused on 5 states, yet as of 2019, 44 states have integrated their benefits delivery with at least two benefit types, while 13 have fully integrated 4 or more federal social service benefits into one application, delivery system, and management system.<sup>101</sup>

These facts have led to the formulation of this testable hypothesis of analysis:

Since US states can provide an integrated-benefits common application, delivery system, and management system for disparate benefit types, victims of identity fraud should be able to seek redress from federal benefits delivery organizations through the same means.

### 4.5.2 Federal Government Implementation

Similar systems include:

1. Consumer Sentinel Network – For law enforcement coordination of identity fraud Consumer Sentinel is an investigative cyber tool that provides members of federal, state, and local law enforcement access to criminal reports about consumer scams and identity theft and fraud related to federal benefit programs.<sup>102</sup> Consumers submit reports when making claims on the FTC website and other reports are provided by data contributors.
2. Organized Crime Drug Enforcement Task Forces (OCDETF) – OCDETF is the largest anti-crime task force in the country. OCDETF is an independent component of the DOJ established to combat transnational-organized-crime and to reduce the availability of

---

<sup>99</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.

<sup>100</sup> Ibid.

<sup>101</sup> Code for America, "Bringing Social Safety Net Benefits Online Examining online platforms for all 50 states." Last modified August 2019. Accessed March 09, 2023. <https://www.codeforamerica.org/features/bringing-social-safety-net-benefits-online/>.

<sup>102</sup> [6]

illicit narcotics in the nation by using a prosecutor-led, multi-agency approach to enforcement. OCDETF leverages the resources and expertise of its partners in concentrated, coordinated, long-term enterprise investigations of transnational organized crime, money laundering, and major drug trafficking networks.<sup>103</sup> OCDETF implements a nationwide strategy combining priority targeting, coordination, intelligence sharing, and directed resourcing to have the greatest impact disrupting and dismantling command and control elements of criminal organizations.

## 4.6 The Benefits of Utilizing a Common Process Platform

This analysis now turns to the benefits of utilizing a common business process across the benefits delivery space and further shows that standardizing and enumerating a series of business lifecycle functions, activities, business capabilities, business use cases, and standardized data elements has specific benefits as outlined in the Federal Integrated Business Framework (FIBF) approach.<sup>104</sup> According to the President's Management Agenda (PMA) of 2019, "State governments, nonprofits, and businesses (including more than 90% of Fortune 500 companies) have reduced costs and improved effectiveness by adopting shared services. By driving standards in capabilities, data, business processes and technology to streamline administrative activities, leaders in these fields have found the greatest gains in efficiency."<sup>105</sup>

This section of the report demonstrates how utilizing a common business process will help Federal government agencies achieve the following six benefits:

1. Leveraging best practices across agencies,
2. Capturing economies of scale,
3. Shortening claim resolution timeframes,
4. Alleviating common victim frustrations,
5. Alleviating common employee frustrations and,
6. Meeting the current administration's PMA and Executive Order (EO) 14058, titled transforming federal customer experience and service delivery to rebuild trust in government.

### 4.6.1 Leveraging Best Practices

This report has established that despite the constraints of their unique statutory and regulatory landscape, benefits delivery agencies have common capability needs as it pertains to federal redress processes. Furthermore, this report frames the federal identity fraud redress process as one enterprise to develop both a common business framework (see section 4.1), and a common

---

<sup>103</sup> [5]

<sup>104</sup> The Federal Integrated Business Framework (FIBF) is a model that enables the Federal government to better coordinate and document common business needs across agencies, focusing on outcomes, data, and cross-functional end-to-end business processes.

<sup>105</sup> Office of Shared Solutions and Performance Improvement. "Centralized Mission Support Capabilities for the Federal Government." Shared Services. Last modified March 2020. Accessed March 9, 2023. <https://ussm.gsa.gov/assets/files/SQS-Public-FAQs-April-2020.pdf>.

business platform (see Section 4.3). However, in the current environment, each agency operates in silos and conducts aspects of its business differently by utilizing different processes and tools to achieve common desired outcomes. In some instances, agencies do not have an existing identity fraud redress program in place outside of their OIGs (e.g., SBA and SSA), while others have clearly articulated rules for how individuals can seek redress from the agency (e.g., the IRS and the VA). The FTC, for example, has endeavored to use a one-stop shop system for law enforcement purposes through the Consumer Sentinel system, which is available to all law enforcement entities, not for comprehensive victim assistance and coordination.

Another example of this siloed approach is at the IRS where the Taxpayer Protection Program (TPP) utilizes a “multi-pronged approach” to identity theft prevention to alleviate the case load of individuals seeking redress. By using “link analysis [to identify] various patterns and trends that might not be picked up by [existing filters].”<sup>106</sup> IRS and SSA currently use these types of preventative capabilities, but they are less prevalent with other benefits delivery agencies. Leveraging best practices will promote process optimization across all agencies by replicating proven and effective practices.

#### **4.6.2 Capturing Economies of Scale**

Moving from a siloed operation where agencies administer separate redress programs to a common business platform that views the federal redress process as one enterprise will promote economies of scale from the utilization of common policies to shared IT and business services. According to the Organization of Economic Cooperation and Development (OECD), economies of scale “refer to the phenomenon where the average costs per unit of output decreases with the increase in scale of magnitude of the output being produced.” By merging certain activities such as vendor services and reporting capabilities, the fixed cost of those activities will reduce the per claimant cost of processing an application.<sup>107</sup> In a research paper published in the journal *Government Information Quarterly* Gouscos et al. argue that “lowering of unit costs for administrative transactions, combined with increased visibility of services that form part of one-stop offerings, provides favorable conditions for increasing transaction volumes.”<sup>108</sup> In summary, sharing the fixed costs of processing federal identity theft redress claims by pooling the increased volume of claimants with common vendor will help alleviate administrative fiscal burdens of operating these programs. This finding is in line with the guiding principle which calls for redress programs to minimize impacts to current operations and budgets.

#### **4.6.3 Shortening Claim Resolution Timeframes**

CBPP and Code for America have partnered with other public benefits corporations and states to run *The Integrated Benefits Initiative* across multiple states, and they have been tracking data on the quantifiable benefits that come with using a consolidated business model utilizing technology to automate processes.<sup>109</sup> Michigan, having participated in this initiative, has seen substantively

---

<sup>106</sup> Senior Internal Revenue Service Official. Videoconference interview by the author. McLean, VA. November 07, 2022.

<sup>107</sup> Gouscos, Dimitris, Manolis Kalikakis, Maria Legal, and Soumi Papadopoulou. "A General Model of Performance and Quality for One-Stop E-Government Service Offerings." *Government Information Quarterly* 24, no. 4 (October 2007): 860-85.

<sup>108</sup> Ibid.

<sup>109</sup> Fujita, Megumi K., Josh LeFevre, Samir Salifou, and Joshua I. Schwartz. *Integrated Benefits Delivery: An Environmental Scan of Current Systems in the United States and around the Globe*. McLean, VA: MITRE, 2021.



significant positive impacts on its benefits delivery system as identified in Figure 4-6. These impacts included a 77% reduction in the application time, an increase of 17% in the approval rate, and a 15% reduction in the days to determination of eligibility.<sup>110</sup> Although this report is not making the assertion that existing redress programs will see comparable benefits, these numbers indicate that process integration, leveraging best practices and systems automation have led to shortening the benefits delivery timeframe in comparable instances.

#### Pilot 1: The Digital Assister

## The Impact from Piloting the Digital Assister

We tracked three primary success metrics over the course of the pilot. The digital assister demonstrated improvements across all three metrics.



**Figure 4-6 The Impacts of Automation and Using a Common Business Platform in Michigan<sup>111</sup>**

### 4.6.4 Alleviating Common Victim Frustrations

Section 2.1 of this report highlights the common frustrations expressed by victims of identity theft. These frustrations centered around the following themes:

1. The burdensome need for the victim to navigate the siloed federal redress processes where they exist and submit multiple applications where necessary.

<sup>110</sup> Civilla and Code for America, “Streamlining Access to Public Benefits in Michigan: Designing a User-Centered Digital Enrollment Experience.” 2019. Accessed March 27, 2023. [http://s3-us-west-1.amazonaws.com/codeforamerica-cms1/documents/Streamlining-Access-Report\\_Integrated-Benefits-Initiative-Civilla\\_Code-for-America\\_March-2019.pdf](http://s3-us-west-1.amazonaws.com/codeforamerica-cms1/documents/Streamlining-Access-Report_Integrated-Benefits-Initiative-Civilla_Code-for-America_March-2019.pdf)

<sup>111</sup> Ibid.

2. The lack of inclusive, equitable, and secure service channels to accommodate all demographics who are victims of identity theft.

Viewing the federal redress process as one enterprise, with a single front door that serves as a one-stop shop, will alleviate these two concerns as well as meet the guiding principles outlined in Section 3.

#### **4.6.5 Alleviating Common Government Employee Frustrations**

Section 2.2 of this report highlights the common frustrations expressed by government officials who interact with the victims of identity theft. These frustrations centered around the following three themes:

1. The lack of established identity theft redress processes within certain institutions.
2. The lack of standardization of thresholds and policies when those policies exist.
3. The need for dedicated funding for redress programs to ensure prioritization.

Viewing the federal redress process as one enterprise, instead of several silos, will alleviate these three concerns as well as meet the guiding principles outlined in Section 3 by providing the capabilities outlined in Section 4.3.

#### **4.6.6 Meeting the Intent of the Current Administration's PMA and Executive Order (EO) 14058**

Increasing trust in government through effective management of government institutions is a critical component of the current administration's Presidential Management Agenda (PMA). In the PMA, the administration states that the manner in which "the public interacts with government programs and benefits influences their level of trust in Government as an institution. [...] Delivering results and being accountable for [public sector] actions will steadily rebuild trust between the public and their government."<sup>112</sup> In an effort to operationalize the PMA, the current administration issued EO instructing federal agencies to take certain actions to build trust in government. EO 14058, titled *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*, identifies 34 high impact agencies, inclusive of all the agencies that fall within the scope of this analysis. This EO, for example, directs the Commissioner of the Social Security Administration:

1. To develop a mobile-accessible, online process so that any individual applying for or receiving services from the Social Security Administration can upload forms, documentation, evidence, or correspondence associated with their transaction without the need for service-specific tools or traveling to a field office,
2. To the maximum extent permitted by law, support applicants and beneficiaries to identify other benefits for which they may be eligible and integrate Social Security Administration data and processes with those of other Federal and State entities whenever possible.<sup>113</sup>

---

<sup>112</sup> The President's Management Council. *The Biden-Harris Management Agenda Vision Toward an Equitable, Effective, and Accountable Government that Delivers Results for All*. Washington, DC: Office of Management and Budget, 2021.

<sup>113</sup> Exec. Order No. 14058, 86 Fed. Reg. 71357 (Dec.16, 2021). Accessed June 25, 2022.  
<https://www.federalregister.gov/documents>.

*“[the manner in which] the public interacts with Government programs and benefits influences their level of trust in Government as an institution [...] delivering results and being accountable for [public sector] actions will steadily rebuild trust between the public and their government.”<sup>114</sup> – The Presidential Management Council*

---

EO 14058 applies to most federal benefits agencies, not just SSA. Each agency of interest for this report fell within the scope of EO 14058. Federal benefits agencies provide fundamental services that not only support their individual missions, but additionally work to foster and promote the American social contract. The evidence presented thus far indicates that these agencies are well-suited to utilize a common business platform that would allow all agencies to meet the spirit and intent of this EO.

## 4.7 Use Cases

As part of this study, several use cases (detailed in Appendix C) were developed to reflect the business processes that a one-stop solution should provide as part of a redress solution. Use cases represent typical processing that would occur as part of the process including the following:

- Interactions between individuals and the organization providing redress
- Events to be accomplished by the organization
- Information to be received, processed and/or provided.

Use cases are agnostic as to whether the events in the business use case are automated, semi-automated, or manually accomplished.

---

<sup>114</sup> The President’s Management Council. *The Biden-Harris Management Agenda Vision Toward an Equitable, Effective, and Accountable Government that Delivers Results for All*. Washington, DC: Office of Management and Budget, 2021.

## 5 Key Considerations

In this section, the report defines the key considerations essential to the implementation of a re-imagined redress program. The considerations are broken out into short-, mid-, and long-term considerations. They will include strategic and where applicable, tactical considerations to establish a federal benefit redress program.

### 5.1 Short-Term Considerations

The following considerations are steps that government can take immediately to move toward an enterprise perspective of the federal redress process. The immediacy of this action lies in the White House's ability to issue executive orders that initialize these processes. In this section we will highlight the consideration, then provide a suggestion of which organization could administer the consideration, and finally some initial steps on how the consideration could be materialized.

#### 5.1.1 Establish Common Thresholds and Processes

Establishing thresholds and process would require the federal government to establish a common lexicon for how to address identity fraud across the federal enterprise and establish benchmark levels that trigger an investigation. Similar to the current administration's approach in EO 14008 on *Tackling the Climate Crisis at Home and Abroad*, the White House could signal the importance of the need for a redress process by "taking a government-wide approach"<sup>115</sup> and convening the relevant government agencies and departments into a federal Identity Fraud Task Force (e.g., IRS, SSA, DOL, SBA, VA). This task force should set guidelines around authorities and responsibilities of agencies and victims. Furthermore, the Task Force could spearhead agencies efforts' by begin to identify and plan for solutions and operational change by documenting:

- specific organization and location information, which defines the entities/people that will perform the functions, processes, and activities, and specifies where the functions, processes, and activities will be performed;
- data/information that would be used by the functions, processes, and activities;
- physical descriptions of systems or applications they believe will need to be developed or acquired;
- the physical infrastructure (e.g., hardware and systems software) that will be needed to support the redress programs; and
- the organizations that will be accountable for security and their roles and responsibilities, including technology standards.

To ensure the viability of the institutional changes described herein, OMB could instruct agencies to establish the processes and rules by which the newly developed identity fraud redress program will operate. Outside of providing the operational guidelines of the program, these

---

<sup>115</sup> Exec. Order No. 14008, 86 Fed. Reg. 7619 (Feb. 1, 2021).

policy documents would ensure the programmatic permanence of the outlined changes, as well as allow for continuity of operations with changing administrations.

To this end, OMB could instruct agencies to develop the following policy documents in line with the thresholds and processes developed by the federal Identity Fraud Task Force and consistent with the Payment Integrity Information Act (PIIA):

1. *A Claimant-Centric Redress Directive*. This policy document will be the overarching guidance establishing the integrated redress programs in each agency. The Directive will include:
  - a. A clear purpose statement defining the authorities from which the author of the document is drawing to establish the program.
  - b. An applicability statement explaining who the document will impact within the agency.
  - c. Clearly defined policy goals of the identity fraud redress programs.
  - d. A mission statement for the identity fraud redress programs.
2. *Claimant-Centric Identity Fraud Redress Program Standard Operating Procedures (SOP)*. Agencies will create SOPs in line with their scope of authority, defining the step-by-step instructions for how to execute the newly established identity fraud redress program. These desk procedures will be at the tactical level of operations and will serve as “cookbooks” on how to properly execute program. The SOPs will include:
  - a. A clearly defined purpose of the job function operating within the identity fraud redress programs.
  - b. Step-by-step instructions on how to operate the tools used in the identity fraud redress program (e.g., Customer Relationship Management tools, or data management tools).

An Identity Fraud Task Force could spearhead agencies efforts' by beginning to identify and plan for solutions and operational changes and documenting:

- a. specific organization and location information, which defines the entities/people that will perform the functions, processes, and activities, and specifies where the functions, processes, and activities will be performed;
- b. data/information that would be used by the functions, processes, and activities;
- c. physical descriptions of systems or applications they believe will need to be developed or acquired;
- d. the physical infrastructure (e.g., hardware and systems software) that will be needed to support the redress programs;
- e. the organizations that will be accountable for security and their roles and responsibilities, including technology standard, and
- f. performance metrics.

### **5.1.2 Establish Inter-Agency Agreements on Data Sharing**

In line with the guiding principles outlined herein, federal benefits agencies can create data sharing agreements with other federal benefits agencies to start the process of streamlining the redress process. The White House could instruct federal benefits agencies to start the process of creating a memorandum of agreement (MOA) or a memorandum of understanding (MOU) with respect to data sharing consistent with applicable laws and regulations. This order would be in line with EO 14058 on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*.<sup>116</sup> By instructing federal agencies that, to the maximum extent permitted by law, they should integrate data systems and processes with those of other Federal and State entities.

### **5.1.3 Make All Service Channels Available**

As identified herein, service channels have the capacity to make the new redress process equitable and inclusive. OMB could instruct agencies to make their full suite of service channels available for the redress process. Where some service channels are not available at specific agencies, the administration should encourage agencies, to the maximum extent permitted by law, to share resources ensuring that victims of identity fraud have equitable access to the redress process. This tactic would be similar to the approach used by Services Australia called *no wrong door*. During an interview conducted for this report representatives from Services Australia stated that “if someone is a victim of identity compromise, they can contact [a state or commonwealth government agency], an [approved] not-for-profit organization, or [approved] private entities like ID Care. It doesn’t really matter where they come in; they come in once and then they’re warm transferred [to the] relevant door they need to go through.”<sup>117</sup> Though Services Australia partners with private entities and not-for-profits, the federal government could start by leveraging all available federal service channels to victims. As an intermediary step to a fully developed one-stop shop process, the *no wrong door* process would allow victims of identity fraud to use any of the many service channels already currently offered by federal agencies.

## **5.2 Mid-Term Considerations**

The following considerations are steps government can take over the course of the next six months to move toward an enterprise perspective of the federal redress process. In this section we will highlight the consideration, then provide a suggestion of which organization could administer the consideration, and finally some initial steps on how the administrator could implement this consideration.

### **5.2.1 Conduct a Macro Economic Benefit-cost Analysis**

Implementing the capabilities outlined in this report will require the investment of financial and human capital. To fully understand the return on investment for the American public, OMB should conduct a macro economic benefit-cost analysis (BCA) of a one-stop shop redress process. The BCA should clearly articulate and quantify categories of benefits associated with making this investment (e.g., cost savings due to shared services, time saved by victims), and the

---

<sup>116</sup> Exec. Order No. 14058, 86 Fed. Reg. 71357 (Dec. 13, 2021).

<sup>117</sup> Services Australia Representative. Videoconference interview by the author. McLean, VA. April 11, 2023.

direct costs of implementation (e.g., the human capital associated with the increased programs). The BCA should also provide a sensitivity analysis to account for margins of error. Furthermore, the BCA should also bifurcate between macro-economic systemic costs and benefits from the micro-economic costs and benefits for the individual agencies.

## **5.2.2 Develop a Whole-of-Government Redress Governance Model**

Moving from a siloed operating posture to an integrated one-stop shop style system requires the development of the proper institutional mechanisms that break down silos. One such tool is the use of inter-agency advisory boards chaired by OMB.

OMB could develop the following claimant-centric governance model which operates in an ongoing iterative process.

1. OMB could instruct Agency heads to craft a unified strategic vision of a claimant-centric identity fraud customer experience. This will unify Agency leaders and the program teams toward a shared vision of a claimant-centric redress program as being integral to the successful execution of that Agency's mission. Similar to section 211 of EO 40008 the White House could instruct "the head of each agency shall submit a draft action plan to the Task Force [...] within 120 days of the date of this order that describes steps the agency can take with regard to its facilities and operations to bolster adaptation and increase resilience to the impacts of climate change."<sup>118</sup> In developing this unified vision, the Agencies must think across the enterprise, and frame the user experience in a manner where the newly developed customer experience program becomes a fundamental component of the victim's assistance culture across the federal enterprise.
2. OMB could issue guidance to benefits delivery Agency directors to embed a claimant-centric redress model into their governance models by advising the Agency heads to select quick wins for initial focus. These quick wins will allow the agency to start small by identifying fundamental areas of the customer experience where the program leads can show quick tangible success. These successes will engender a sense of accomplishment and will promote buy-in to this new claimant-centric governance model for both operational and tactical level personnel.
3. OMB could create an inter-agency identity fraud customer experience board comprised of the directors of the newly created Identity fraud redress offices, a set of rotating front-line staff who interact with victims of identity fraud (temporary membership that rotates annually), and identity fraud victim-advocate groups. This board will develop guidance for identity fraud programs by leveraging identity fraud customer experience best practices across government. This board will serve as a matrix-style organizational structure. The board will have advisory authorities as prescribed by OMB and will report back to OMB on how to improve the claimant-centric process.
4. OMB, in collaboration with the identity fraud customer experience board, could develop key performance indicators (KPIs) for the customer experience program. They could also establish a common lexicon and set of thresholds for benefits delivery agencies to process these claims. OMB would use these metrics as evaluative measures for the success of the claimant-centric redress program and publish an annual report card for each agency.

---

<sup>118</sup> Exec. Order No. 14008, 86 Fed. Reg. 7619 (Feb. 1, 2021).

OMB will evaluate the KPIs annually and readjust them based on the success of the program.

### 5.2.3 Run Communication Campaigns

As identified herein, discovering that you are a victim of identity fraud is a traumatizing experience according to individuals interviewed for this report.<sup>119</sup> These victims have called the current redress process, “burdensome, messy, confusing, isolating, and frustrating.”<sup>120</sup> According to the PRAC, “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.”<sup>121</sup> Part of alleviating this sense of isolation is ensuring that victims of identity theft know how to seek redress. The reimaged redress process described herein would be ineffective if the intended cohort of interest does not know how to access the integrated process. To this end, the FTC, as the current operator of [identitytheft.gov](https://www.identitytheft.gov), could be responsible for running communications campaigns to inform the government.

Benefits delivery agencies need to educate the potential registrant of the availability of that program’s benefit. Whether done proactively or passively, there is a requirement to communicate the availability of the redress processes to the public. Inputs for this process include messages, communication tools, and active searches.<sup>122</sup> Outputs for this phase of the lifecycle include identifying the intended population groups and ensuring they understand the program.<sup>123</sup>

In the *American Journal of Public Health*, Anand Parekh identified the lessons learned for the ACA by identifying a need for multi-level communication, and a need for steady incremental communication.<sup>124</sup> Multilevel communication would include “not only general messages for the mass audience but also targeted messages at the group level and tailored messages at the individual level.”<sup>125</sup> Given the diversity of the demographics of identity fraud identified herein, an equally diverse level of communication is required to target those populations. Notably, in its 2021 survey, the U.S. Census found that over 67 million Americans aged five years and older speak a language other than English at home.<sup>126</sup> Furthermore, there is an opportunity to partner with credit reporting agencies to allow them to serve as a pipeline of reporting for potential identity fraud cases. Many consumers receive credit reports and other credit related information from the credit bureaus and know how to reach them for any identity fraud related matters. With respect to steady, incremental communications the agencies would have to adopt a consistent and sustained message around Identity Fraud. This is why it would be important for Congress to allocate dedicated funding for identity fraud redress programs.

---

<sup>119</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>120</sup> National Victim's Advocate. Videoconference interview by the author. McLean, VA. November 3, 2022.

<sup>121</sup> Executive Council of the Inspectors General on Integrity and Efficiency. Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs. By Pandemic Response Accountability Committee. Washington, DC: PRAC, 2022.

<sup>122</sup> K. Lindert, T. G. Karippacheril, I. R. Caillava, and K. N. Chávez, eds., *Sourcebook on the Foundations of Social Protection Delivery Systems*, Washington, DC: World Bank, 2020. doi:10.1596/978-1-4648-1577-5. License: Creative Commons Attribution CC BY 3.0 IGO.

<sup>123</sup> Ibid.

<sup>124</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5388982/>

<sup>125</sup> Ibid.

<sup>126</sup> <https://data.census.gov/table?tid=ACSDP5Y2021.DP02&hidePreview=true>



## 5.3 Long-Term Considerations

The following considerations are steps the government can take over the course of the next 12 months to move toward an enterprise perspective of the federal redress process. In this section we will highlight the consideration, then provide a suggestion of which organization could administer the consideration, and finally some initial steps on how the consideration could be materialized.

### 5.3.1 Apply the Federal Integrated Business Framework (FIBF)

OMB could request that the General Services Administration (GSA), through the Office of Shared Solutions and Performance Improvement (OSSPI), commission a detailed assessment using the Federal Integrated Business Framework (FIBF) to standardize and enumerate federal redress business lifecycle functions, activities, business capabilities, business use cases, and data elements.<sup>127</sup> In 2019, the Director of OMB issued a memorandum to the heads of executive departments and agencies titled “Centralized Mission Support Capabilities for the Federal Government.” This issuance instructed heads of federal agencies that “the Government will establish a process to identify mission support functions suitable for sharing based on cross-agency agreement on targeted outcomes and service delivery standards.”<sup>128</sup> The memorandum further states that, “the standards will follow the FIBF to identify a common set of capabilities for designated mission-support functions.”<sup>129</sup> The standards are intended for inter-agency collaboration, they may inform a path to implementation for the benefits delivery agencies. According to OSSPI, “business standards, established and agreed to by agencies, using FIBF enable the government to better coordinate on the decision-making needed to determine what can be adopted and commonly shared. They are an essential first step towards agreement on outcomes, data, and cross-functional end-to-end processes that will drive economies of scale and leverage the government’s buying power.”<sup>130</sup>

The FIBF includes the following five components:

1. **Federal Business Lifecycles, functional areas, functions, and activities** serve as the basis for a common understanding of what services agencies need and solutions that should be offered.<sup>131</sup> This report has provided a basis for this component.
2. **Business Capabilities** are the outcome-based business needs mapped to Federal government authoritative references, forms, inputs, outputs, and data standards.<sup>132</sup> This report has provided a basis for this component.

---

<sup>127</sup> The Federal Integrated Business Framework (FIBF) is a model that enables the Federal government to better coordinate and document common business needs across agencies, focusing on outcomes, data, and cross-functional end-to-end business processes.

<sup>128</sup> Vought, Russell T. Memorandum, “Memorandum for Heads of Executive Departments and Agencies,” April 26, 2019. <https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf>.

<sup>129</sup> Ibid.

<sup>130</sup> General Services Administration. “Mission Support Business Standards.” GSA.gov. Accessed March 27, 2023. <https://ussm.gsa.gov/fibf/#How-are-the-Business-Standards-Used>.

<sup>131</sup> Ibid.

<sup>132</sup> Ibid.

3. **Business Use Cases** are a set of agency “stories” that document the key activities, inputs, outputs, and other line of business intersections to describe how the Federal government operates.<sup>133</sup> This report provides a foundation for this component.
4. **Standard Data Elements** identify the minimum data fields required to support the inputs and outputs noted in the use cases and capabilities.<sup>134</sup>
5. **Service Measures** define how the government measures successful delivery of outcomes based on timeliness, efficiency, and accuracy targets.<sup>135</sup>

### 5.3.2 Fusion Center for Investigations

Developing a national response to address identity fraud requires a modified approach to the sharing of information and intelligence. Leaders must move forward with a new paradigm on the exchange of information and intelligence, one that includes the integration of law enforcement, public safety, and the private sector. Fusion Centers provide the capability for the collaborative sharing of information amongst law enforcement, public safety, and the private sector to increase the ability to detect, prevent, and solve crimes.<sup>136</sup>

### 5.3.3 Congressional Action

This report started from the foundational premise that seeking redress from the federal government should be a seamless process where the claimant (the victim of a crime) can request an investigation into their claim and, if the facts support their claim, be brought to a pre-injury condition. Though the Executive branch of government has a role in the administration and execution of a redress program, it would be within the US Congress’ authority to codify the existence of these programs and allocate the funding for their execution. This report has laid out a conceptual basis for action required from the US government to execute on the vision laid out herein. Congress could use guiding principles outlined in Section 3 of this report as the basis for legislation around a reimagined federal identity fraud redress system. As elucidated in Section 2, the demographics of identity fraud touch every cohort of Americans equally. Congress has a clear interest in addressing these concerns. Delivering results to victims of identity fraud is at the core of rebuilding trust in government institutions and reinforcing the legitimacy of public institutions.

Beyond the guiding principles outlined herein, Congress needs to re-examine the existing barriers that inhibit agencies from sharing identity fraud data related to those specific claims (e.g., IRS does not share data due to legal constraints established through 26 USC 6103). In an interview with a senior IRS official, when asked whether there is a need for legislative change, the senior official said, “I always thought it would be legislative. I don't know what OMB can do [without congressional action to allow IRS to share information]. I thought that we would need [something] similar to the expansion of our disclosure provisions to participate in the [Identity Theft Tax Refund Information Sharing and Analysis Center] (ISAC). [That collaboration] did require legislative activity [through the] Taxpayer First Act. So, from my vantage point, I always

---

<sup>133</sup> Ibid.

<sup>134</sup> Ibid.

<sup>135</sup> Ibid.

<sup>136</sup> Ibid.

thought it had to be legislative to change the actual codes that we operate under, which is generally 6103 for the IRS.”<sup>137</sup> The legislative changes required to the tax code to allow for interagency data sharing relating to identity fraud could be crafted in a manner similar to legislation around tax information sharing for student loans and financial aid. When speaking to this point the senior IRS official further stated that, “There is actually legislation that directed that particular data exchange to reduce the burden of taxpayers applying for student loans and financial aid, so it's a limited purpose but a specific purpose with specific information that will be exchanged [...] that particular legislation also directed the agencies to create an online portal that integrated this information exchange with the backbone being basic income information such as the amount of the adjusted gross income and other information. It's not everything around that return [rather] very specific[information] for a specific purpose.”<sup>138</sup>

---

<sup>137</sup> Senior Internal Revenue Service Official. Videoconference interview by the author. McLean, VA. November 07, 2022.

<sup>138</sup> Ibid.

## Appendix A Acronyms

<b>ACA</b>	Patient Protection and Affordable Care Act
<b>ACSC</b>	Australian Cyber Security Centre
<b>AI</b>	Artificial Intelligence
<b>API</b>	Application Programming Interface
<b>ARPA</b>	American Rescue Plan Act
<b>BCA</b>	Benefit-Cost Analysis
<b>BJS</b>	Bureau of Justice Statistics
<b>CBPP</b>	Center for Budget and Policy Priorities
<b>CARES Act</b>	Coronavirus Aid, Relief, and Economic Security Act
<b>CDC</b>	Centers for Disease Control and Prevention
<b>CIGIE</b>	Council of the Inspectors General on Integrity and Efficiency
<b>COVID-19</b>	Novel Coronavirus Disease 2019 (SARS-CoV-2)
<b>DC</b>	District of Columbia
<b>DOJ</b>	Department of Justice
<b>DOL</b>	Department of Labor
<b>EIDL</b>	Economic Injury Disaster Loan Letter
<b>EO</b>	Executive Order
<b>FBI</b>	Federal Bureau of Investigations
<b>FIBF</b>	Federal Integrated Business Framework
<b>FSB</b>	Federation of Small Businesses
<b>FTC</b>	Federal Trade Commission
<b>GAO</b>	Government Accountability Office
<b>GRM</b>	Grievance Redress Mechanism
<b>GSA</b>	General Services Administration
<b>HHS</b>	U.S. Department of Health and Human Services
<b>IRS</b>	Internal Revenue Service
<b>IDTVA</b>	Identity Theft Victim Assistance
<b>ISAC</b>	Identity Theft Tax Refund Information Sharing and Analysis Center
<b>IT</b>	Information Technology
<b>ITRC</b>	Identity Theft Resource Center

<b>KPI</b>	Key Performance Indicator
<b>LEO</b>	Law Enforcement Organization
<b>LIHEAP</b>	Low-Income Home Energy Assistance Program
<b>MOA</b>	Memorandum of Agreement
<b>MOU</b>	Memorandum of Understanding
<b>NICS</b>	National Instant Criminal Background Check System
<b>N/A</b>	Not Available
<b>OAIC</b>	Office of the Australian Information Commissioner
<b>OCDETF</b>	Organized Crime Drug Enforcement Task Forces
<b>OIG</b>	Office of Inspector General
<b>OMB</b>	Office of Management and Budget
<b>PEUC</b>	Pandemic Emergency Unemployment Compensation Program
<b>PIIA</b>	Payment Integrity Information Act of 2019
<b>PII</b>	Personally Identifiable Information
<b>PMA</b>	Presidential Management Agenda
<b>PPP</b>	Paycheck Protection Program
<b>PRAC</b>	Pandemic Response Accountability Committee
<b>SARS</b>	Severe Acute Respiratory
<b>SMS</b>	Short Message Service
<b>SBA</b>	Small Business Administration
<b>SNAP</b>	Supplemental Nutrition Assistance Program
<b>SOP</b>	Standard Operating Procedures
<b>SSA</b>	Social Security Administration
<b>SSN</b>	Social Security Number
<b>TPP</b>	Taxpayer Protection Program
<b>USC</b>	U.S. Code
<b>USDA</b>	U.S. Department of Agriculture
<b>U.K.</b>	United Kingdom
<b>VA</b>	US Veterans Affairs Administration
<b>WHO</b>	World Health Organization

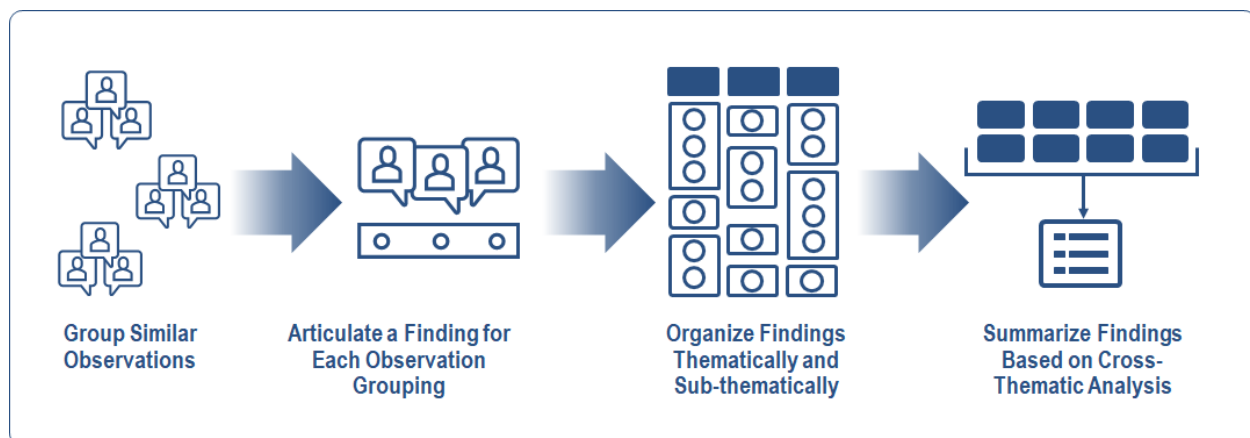
# Appendix B Methodology

## Environmental Scan

### Overview

This report provides valuable information to key stakeholders, including the public, Congress, executive branch agencies, and agencies administering federal benefit programs on design elements to reimagine a federal identity fraud redress program. MITRE's environmental scan leveraged a variety of information sources to characterize the current landscape, highlight challenges and obstacles, and identify areas for improvement.

MITRE used a qualitative data-gathering protocol to capture the factors that affected the outcomes of victims of identity fraud by examining the execution of federal benefit programs and their processes, governance, and technology involved in providing any redress to victims. The protocol provided a systematic approach to discover and document the challenges, successes, and opportunities raised during MITRE's interviews and document review. MITRE conducted the analysis in four steps as shown in the figure below.



**Figure B-1 Evaluation Methodology**

The analysis process synthesizes information gathered from stakeholder interviews and document reviews. Initially, observations are gathered from these data sources. Observations are specific facts drawn from the document review or interview comments; they are directly attributable to a particular data source. The team categorizes and collates the observations into broader findings and themes and uses these to highlight best practices, lessons learned, and optimal approaches for implementing a reimagined federal redress program. Findings are key inferences drawn from the observations. Themes are high-level concepts that recur across multiple findings; themes group findings to communicate the broadest analytical takeaways.

The team then applied evidence-based design principles to identify examples based on the findings and what relevant, credible examples already exist and the validity of the examples. The team translated the relevant evidence into design criteria (key considerations) that can be used to guide the development to improve the federal redress program and outcomes for victims of identity fraud.

This page intentionally blank.

# **Appendix C Use Cases**

## **C.1 Initial Contact With Agency**

**End-to-End Business Process:** Requests for Federal Benefit Redress from Agency

### **Business Scenario Covered**

Initial Identity Fraud Claim with Benefit Agency

### **Business Actors**

- Victim
- Federal Benefit Agencies
- FTC

### **Synopsis**

A currently employed hospital worker receives a letter from their State Workforce Agency (SWA) stating s/he has been awarded unemployment insurance benefits. The individual notifies their employer Human Resources department to get the matter resolved. However, unfortunately, four months later the employee is notified they are a part of a layoff and seeks unemployment insurance benefits to discover they have been denied benefits due to ineligibility.

### **Assumptions and Dependencies**

1. There are three methods to correspond with agencies within the re-imagined redress “one-stop” shop approach including in-person, telephone and digital (mobile device or internet).
2. Supporting information to file for unemployment insurance is available to the victim and are digitally available to the SWA.
3. All predecessor activities required to trigger the Initiating Event have been completed.
4. The one-stop shop platform has been stood up with all agencies able to leverage the suite of capabilities.
5. Victim has all information to complete the identity fraud claim.
6. There are sufficient resources to provide the service.



## Initiating Event

Victim requests benefit re-instatement

## Typical Flow of Events

**Table C-1. Typical Flow of Events for Initial Contact with Agency**

#	Redress Event	Non-Redress Event*	Input(s)	Output(s) / Outcome(s)
1	-	<ul style="list-style-type: none"> <li>a) Requests re-instatement of eligibility for unemployment insurance.</li> <li>b) Requests protection of personally identifiable information (PII).</li> <li>c) Requests counseling to cope with stress of identity theft.</li> </ul>	Caller contact information; fraud incident claim information; data about the victim.	<ul style="list-style-type: none"> <li>• Submitted identity theft and fraud claim.</li> <li>• Requests for PII protection.</li> <li>• Requests for trauma care support.</li> </ul>
2	<ul style="list-style-type: none"> <li>• Receive and process identity theft and fraud claim.</li> <li>• Receive and process requests for protection of PII.</li> <li>• Receive and process requests for trauma care support.</li> </ul>	-	<ul style="list-style-type: none"> <li>• Submitted identity theft and fraud claim.</li> <li>• Requests for PII protection.</li> <li>• Requests for trauma care support.</li> </ul>	<ul style="list-style-type: none"> <li>• Identity theft and claim response.</li> <li>• PII protection response.</li> <li>• Trauma care support response.</li> </ul>
3		<ul style="list-style-type: none"> <li>• Approve identity theft and fraud claim</li> <li>• Approve PII protection request</li> </ul>	<ul style="list-style-type: none"> <li>• Identity theft and claim response</li> <li>• PII protection response</li> <li>• Trauma care support response</li> </ul>	<ul style="list-style-type: none"> <li>• Approved claim</li> <li>• Approved PII protection</li> </ul>

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843**

		<ul style="list-style-type: none"> <li>• Approve trauma care support request</li> </ul>		Approved trauma care support
4	<ul style="list-style-type: none"> <li>• Received approved claim</li> <li>• Received approved PII protection</li> <li>• Received approved trauma care support</li> </ul>	-	<ul style="list-style-type: none"> <li>• Approved claim</li> <li>• Approved PII protection</li> </ul> Approved trauma care support	<ul style="list-style-type: none"> <li>• Provide identity fraud case management docket</li> <li>• Provide PII protection</li> </ul> Provide trauma care support
5	<ul style="list-style-type: none"> <li>• Route identity fraud case management information to appropriate entities including FTC</li> <li>• Validate PII protection</li> </ul> Confirm trauma care support	-	Identity fraud case management docket	Identity fraud case docket updated

## C.2 Trauma Care Support

**End-to-End Business Process:** Providing trauma-informed care to victims of identity theft and fraud

### Business Scenario Covered

Initial Request for Trauma-Informed Care

### Business Actors

- Victim
- Trauma-Informed Care Service Provider
- Trauma-Informed Care Practitioner
- Federal Benefit Agency Federal Benefit

### Synopsis

A currently employed hospital worker receives a letter from their State Workforce Agency (SWA) stating s/he has been awarded unemployment insurance benefits. The individual notifies their employer Human Resources department to get the matter resolved. However, unfortunately, four months later the employee is notified they are a part of a layoff and seeks unemployment insurance benefits to discover they have been denied benefits due to ineligibility. After initial contact with the federal agency, the victim is referred to a trauma-informed care service provider to begin to restore their wellbeing.

### Assumptions and Dependencies

1. The individual has already established contact with the federal benefit agency seeking redress.
2. All predecessor activities required to trigger the Initiating Event have been completed.
3. The one-stop shop platform has been stood up with all agencies able to leverage the suite of capabilities.
4. The federal benefit agency has an established relationship/partnership agreement with a trauma-informed care service provider.
5. The trauma-informed care service provider has trauma-informed care trained practitioners.
6. The trauma-informed care service provider has established best practices and processes for screening, assessment, case planning, case coordination, secondary consultation, and client feedback.<sup>139</sup>

---

<sup>139</sup> (Government, 2022)

7. There are sufficient resources to provide the service.
8. There is information available in multiple languages.
9. The service is provided at the victim's consent and is confidential.
10. The trauma-informed care service provider has connections with a broader system of support.

## Initiating Event

Victim requests benefit re-instatement.

## Typical Flow of Events

**Table C-2. Typical Flow of Events for Trauma Care Support**

#	Redress Event	Non-Redress Event*	Input(s)	Output(s) / Outcome(s)
1	-	a) Requests counseling to cope with stress of identity theft and fraud.	<ul style="list-style-type: none"> <li>• Caller contact information; fraud incident claim information; data about the victim.</li> <li>• Submitted identity theft and fraud claim.</li> <li>• Approved trauma care support request.</li> </ul>	Victim is assigned a trauma-informed care practitioner.
2	Trauma-informed care practitioner establishes initial contact with victim.	Create Trauma-informed care victim case management record.	<ul style="list-style-type: none"> <li>• Submitted identity theft and fraud claim.</li> </ul>	<ul style="list-style-type: none"> <li>• Identification of immediate resources available to the victim.</li> <li>• Overview of the trauma-informed care process model and where the victim is within the various phases of the model.</li> </ul>

				<ul style="list-style-type: none"> <li>• Trauma-informed care service provider mission statement.</li> <li>• Initial triage assessment of possible outcomes.</li> <li>• Copy of victim rights. Next steps/direction for victim.</li> </ul>
<b>3</b>	Trauma-informed care practitioner requests consent from victim to provide support.	-	<ul style="list-style-type: none"> <li>• Informed consent from victim.</li> </ul> <p>Trauma-informed care victim case management record.</p>	<ul style="list-style-type: none"> <li>• Consent confirmation. Information regarding grievances.</li> </ul>
<b>4</b>	Trauma-informed care practitioner provides intake assessment to establish a victim profile of potential needs based on degree of fraud victimization.	-	<ul style="list-style-type: none"> <li>• Submitted identity theft and fraud claim.</li> <li>• Trauma-informed care victim case management record.</li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality statement.</li> <li>• Generated PIN.</li> <li>• Individualized plan for redress related trauma-informed care</li> <li>• Information on benefits and limits of service based on intake assessment.</li> </ul> <p>Identification of additional support services.</p>

## **C.3 Request Federal Fraud Fusion Center Investigation**

**End-to-End Business Process:** Requests for Criminal Investigation Using a Federal Fraud Fusion Center Security Operations Center (SOC)

### **Business Scenario Covered**

Initial Identity Fraud Investigation

### **Business Actors**

- Victim
- Federal Benefit Agencies
- FTC
- Law Enforcement
- Federal, State and Local Public Safety Organizations

### **Synopsis**

A request is made to initiate an identity fraud investigation based on information collected from victims and other threat intelligence

### **Assumptions and Dependencies**

1. There have been several similar identity fraud incidents effecting multiple victims or a significant fraud incident meeting threshold condition.
2. The amount of the fraud committed meets the threshold for criminal investigation.
3. The Fraud Fusion (Data) Center Security Operations Center (SOC) applies the scanning, analysis, response, and assessment (SARA) model.
4. There are adequate resources including fraud prevention, cybersecurity, threat intelligence and analytics teams.
5. The Fraud Fusion center leverages law enforcement and public safety agencies at the federal, state, and local levels in addition to federal agencies' Office of the Inspector General (OIG).
6. The Fraud Fusion Center SOC includes threat intel, advanced analytics, monitoring, and response operations.
7. There are automated interfaces between functional areas/functions/activities or between provider solutions/systems to promote information sharing when required.

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843**

8. There is no presumption as to which activities are executed by which actor, or which activities are automated, semiautomated, or manual.
9. There is sufficient information to conduct the criminal investigation based on the initial and subsequent fraud incident reports.

## Initiating Event

Fraud incident meets the threshold for cross-agency collaboration and exchange of information and intelligence among law enforcement and public safety agencies at the federal, state, and local levels.

## Typical Flow of Events

**Table C-3. Typical Flow of Events for Request Fusion Fraud Fusion Center Investigation**

#	Redress Event	Non-Redress Event*	Input(s)	Output(s) / Outcome(s)
1	-	a) Requests cross-agency fraud investigation	Fraud incident claim information; data about the victim.	<ul style="list-style-type: none"> <li>• Approved identity theft and fraud claim.</li> <li>• Requests cross-agency fraud investigation</li> </ul>
2	<ul style="list-style-type: none"> <li>• Receive approved identity theft and fraud claim.</li> <li>• Receive additional threat intelligence related to fraud incident.</li> <li>• Receive requests for cross-agency fraud investigation</li> </ul>	-	Pre-investigation assessment	<ul style="list-style-type: none"> <li>• Fraud incident report</li> <li>Formal fraud case</li> </ul>
3	<ul style="list-style-type: none"> <li>• Distribute fraud incident report across multiple agencies as</li> </ul>	<ul style="list-style-type: none"> <li>• Perform fraud analysis</li> </ul>	Fraud analysis	Enhanced fraud incident report

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2843**

	part of data fusion center fraud investigation <ul style="list-style-type: none"> <li>• Issue notice to agencies to collect and preserve data</li> </ul>	<ul style="list-style-type: none"> <li>• Monitor networks for cyber-related fraud activity</li> <li>• Fuse data from multiple data sources</li> <li>• Collect additional supporting evidence</li> <li>• Leverage forensic expertise</li> </ul>		
4	<ul style="list-style-type: none"> <li>• Collect reports and information</li> </ul>	-	<ul style="list-style-type: none"> <li>• Fraud investigation analysis reports</li> </ul> Threat intelligence	<ul style="list-style-type: none"> <li>• Provide final reports</li> </ul> Updated fraud case