Employment Development Department
State of California

Fraud Tools Assessment

Employment Development Department
State of California

Employment Development Department
State of California

Table of Contents

1 Executive Summary

1.1 Context

Assembly Bill 138 (Chapter 78, Statutes of 2021) added Section 340(a)(1) to the California Unemployment Insurance Code (CUIC), requiring the Employment Development Department (EDD) to provide a report to the California State Legislature assessing the effectiveness of the Department's fraud prevention and detection tools. This report satisfies that requirement.

1.2 Confidentiality

As Section 340(b) of the CUIC allows, "Details on fraud methods and tools may be generalized, excluded, or redacted to protect the fraud deterrence practices of the department." To preserve the integrity of the Department's defenses against perpetrators of fraud and cybercrime, the specifics of the plan must remain confidential, as it provides a comprehensive list of desired industry-standard tool features. EDD appreciates the Legislature's discretion in handling these sensitive matters and may provide additional details of the assessment in a private forum upon request.

2 Scope of Assessment

EDD administers two major benefit programs: Unemployment Insurance (UI) and State Disability Insurance (SDI). These programs provide temporary wage replacement benefits to eligible individuals. EDD employs a Department-wide fraud prevention and detection strategy, with the collective intent to safeguard taxpayer funds, while continuing to pay claimants timely.

This assessment takes a comprehensive approach, evaluating not only individual tool capabilities but also their integration with existing systems, compliance with legal standards, and impact on operational efficiency.

The Department-wide fraud prevention and detection strategy employed by EDD includes:

- Identity verification and authentication
- Cross matching and data sharing
- Public awareness campaigns and collaboration with law enforcement
- Coordination with the Fraud Governance Group

Fraud Prevention Components in Scope

Fraud Prevention Component	Description
Identity Verification and Authentication	EDD currently uses ID.me as an identity verification tool. It verifies the identities of claimants who apply through the Department's shared customer portal (SCP), which serves as the public-facing portal for UI and SDI customers. Per the National Institute of Standards and Technology (NIST) 800-63-3 requirements, this service includes document-based and biometrically derived identity verification. ID.me was implemented in October 2020. As part of the EDDNext modernization effort, EDD will introduce Socure as a replacement to ID.me for 10% of UI customers initially and ultimately for 100% of UI and SDI customers. The proposed change is expected to result in an improved customer experience, enhanced data quality, and continued deterrence of fraudulent activities (see page 6).
Fraud Detection Tool	Thomson Reuters (TR) [Pondera and CLEAR Platform] is used by EDD as a fraud detection tool in conjunction with internal screening criteria. TR provides the following services to EDD: • Fraud detection screening; • Business intelligence; and • Investigations management TR screens new UI and SDI customers for non-identity-related fraud risk (e.g., mailing address, county and federal incarceration status). TR is used to enhance EDD's manual process for screening identity-related fraud risk for paper and phone UI claimants. For purposes of this assessment, this report focuses on TR's fraud detection capabilities. TR was implemented in December 2020.

Fraud Prevention Component	Description
Cross Matching and Data Sharing	EDD performs internal fraud mitigation efforts by cross-matching data with the California Department of Corrections and Rehabilitation, Department of State Hospitals, and the Department of Juvenile Justice. EDD participates in the National Association of State Workforce Agencies (NASWA) Integrity Data Hub, which was implemented in June 2023. This multistate data system provides advanced data cross-matching and analysis capability that detects and prevents UI fraud and improper payments. EDD shares UI new claim data and provides daily updates to the Integrity Data Hub. Currently, EDD is reviewing the Integrity Data Hub data and defining business requirements for the next phase of the project.
Public Awareness Campaigns and Collaboration with Law Enforcement	EDD communicates to all stakeholders (public, claimants, employers, physicians/practitioners) how to report fraud, avoid scams, avoid committing fraud, and the penalties and prosecution for providing false information or not reporting information to EDD. This communication is provided at edd.ca.gov/FightFraud In addition, EDD's Response to Fraud page includes statistics on investigations, arrests, and convictions. It features recent news articles and quotes that reinforce EDD's efforts in fraud prevention which also serves as deterrence. EDD has created investigative guides for law enforcement and has offered technical assistance to partners working on fraud-related cases. Regional contacts have been established for each division of the State allowing EDD to work with agencies that need assistance with unemployment fraud cases. EDD has also set up a system where out-of-state state and local law enforcement agencies can obtain information from EDD to investigate and prosecute UI fraud in their jurisdiction.
Governance	EDD's Fraud Governance Group is a key component of the Department's successful fraud prevention efforts. The group effectively coordinates and guides various initiatives, such as identity verification, fraud detection, data sharing, public awareness, and law enforcement collaboration.

3 Identity Verification and Authentication

ID.me is classified as an **identity verification tool** that authenticates a given person's identity via user-provided information, documents, and "selfie" images, or a live virtual interview with ID.me via a trusted referee. Customers may also opt out of the "selfie" image process and not share their biometric information; selfie images and associated biometric data are deleted after 24 hours. EDD requested and received from ID.me the NIST 800-63-3 IAL2 & AAL2 Annual Conformity Review on June 14, 2023.

3.1 ID.me – Mitigated Fraud

The data collected from January 1, 2024, through September 30, 2024, was thoroughly analyzed separately for UI claimants, SDI claimants, and SDI medical providers. During this period, the ID.me platform prevented 7,028 potentially fraudulent UI claims, 2,862 potentially fraudulent SDI claims, and 115 potentially fraudulent SDI medical provider claims from being filed.

<table>
<tr><th colspan="6">January 1, 2024 – September 30, 2024: UI Claimants</th></tr>
<tr><th>Started Verification</th><th>Abandoned[1]</th><th colspan="2">Unsuccessful</th><th colspan="2">Verified</th></tr>
<tr><td rowspan="3">1,152,943</td><td rowspan="3">67,224 (5.83%)</td><td colspan="2">72,707 (6.31%)</td><td colspan="2">1,005,984 (87.25%)</td></tr>
<tr><td>Attempted Trusted Referee</td><td>Did Not Attempt Trusted Referee</td><td>Pre-verified</td><td>Did Not Attempt Trusted Referee</td><td>Self-Service</td></tr>
<tr><td>26,389 (36.3%)</td><td>46,318 (63.7%)</td><td>647,928 (64.4%)</td><td>299,031 (29.7%)</td><td>59,025 (5.9%)</td></tr>
<tr><td colspan="6">Estimated Fraud Prevented: 7,028 Individuals</td></tr>
</table>

<table>
<tr><th colspan="6">January 1, 2024 – September 30, 2024: DI Claimants</th></tr>
<tr><th>Started Verification</th><th>Abandoned</th><th colspan="2">Unsuccessful</th><th colspan="2">Verified</th></tr>
<tr><td rowspan="3">725,264</td><td rowspan="3">32,246 (4.44%)</td><td colspan="2">37,880 (5.22%)</td><td colspan="2">652,189 (87.92%)</td></tr>
<tr><td>Attempted Trusted Referee</td><td>Did Not Attempt Trusted Referee</td><td>Pre-verified</td><td>Did Not Attempt Trusted Referee</td><td>Self-Service</td></tr>
<tr><td>9,547 (25.2%)</td><td>28,333 (74.79%)</td><td>345,398 (52.95%)</td><td>275,982 (42.31%)</td><td>30,809 (4.72%)</td></tr>
<tr><td colspan="6">Estimated Fraud Prevented: 2,949 Individuals</td></tr>
</table>

[1] Individuals who were presented with a path forward in the identity verification process but opted not to proceed.

<table>
<tr><th colspan="5">January 1, 2024 – September 30, 2024: Medical Providers</th></tr>
<tr><th>Started Verification</th><th>Abandoned</th><th colspan="2">Unsuccessful</th><th colspan="2">Verified</th></tr>
<tr><td rowspan="3">7,865</td><td rowspan="3">1,326
(17%)</td><td colspan="2">1,126
(14%)</td><td colspan="2">5,298
(67%)</td></tr>
<tr><td>Self-Service</td><td>Trusted Referee</td><td>Self-Service</td><td>Trusted Referee</td></tr>
<tr><td>1,057
(94%)</td><td>69
(6%)</td><td>5,118
(94%)</td><td>180
(3%)</td></tr>
<tr><td colspan="6">Estimated Fraud Prevented: 115 Individuals</td></tr>
</table>

The estimated volume of fraudulent users that ID.me prevents from completing identity verification is determined through meticulous monitoring conducted by ID.me's Security and Data Analytics teams. This monitoring encompasses the detection of social engineering, synthetic identity theft, and other forms of fraudulent activity across state and federal partners. The identification of fraudulent activity includes the examination of ID.me's fraud flags, the detection of duplicate personally identifiable information, and the supervision of verification attempts.

3.2 Identity Verification – Next Steps

The current contract with ID.me expires in June 2025. As part of EDD's modernization effort, EDDNext, market research, and a competitive bidding process was conducted in 2023 with four identity verification vendors. Socure was selected to replace ID.me's services.

The model used by ID.me as an identity service provider requires new claimants to interact with two separate websites. First, claimants sign-in to myEDD, the Department's shared customer portal. Then, claimants navigate to ID.me's website to verify their identity. Following verification, they must return to myEDD. Some claimants abandon this process and therefore EDD does not have information for these customers.

The new, frictionless identity verification model offered by Socure will enable claimants to verify their identity directly within myEDD, giving EDD more insight into customer abandonment points or process continuation. This transparency allows EDD to collect the data provided by the claimant to minimize data collection requirements in subsequent interactions. If necessary, Socure also supports verification using documents and "selfie" images, or a live virtual interview if needed.

In the first phase of Socure's implementation, 10 percent of UI customers will be directed to verify their identity within the myEDD portal, without the need to navigate to a separate website. This phased approach will allow EDD to study the customer journey and the identity verification data before increasing the percentage of customers using Socure and prior to integration with SDI.

4 Fraud Detection Tool

TR is a **fraud detection tool** that assesses the likelihood of a fraudulent claim using internal and third-party data sources, based on specific parameters. TR information is reviewed on the following parameters:

- Efficacy of existing fraud filters;
- Sources referenced;
- Outputs generated by the tool.

4.1 TR – Mitigated Fraud

The table below represents the number of claims, and the estimated amount of fraud mitigated because of the use of the TR tool. At the time of this report's publication, 2024 data was only available through September 30, 2024.

TR - Calendar Year	UI Fraud Claims Prevented	UI Fraud Mitigated
2024 YTD Total	**5,526**	**$19,325,063**

SDI utilizes TR in a different method compared to UI. SDI reviews claimants and medical providers that have been flagged by TR to examine if appropriate action needs to be taken.

TR - Calendar Year	SDI Fraud Claims Reviewed (Total)	
2024 YTD Total	**5,149**	
	Claimants: 1,828	**Medical Providers: 3,321**

4.2 TR – Next Steps

EDD continues to identify any constraints and limitations within TR provided information regarding its algorithms and business rules documentation, the output assessment, and requirements. EDD continues to review its use of TR to refine techniques and optimize the filters.

5 Cross Matching and Data Sharing

In addition to the TR and ID.me tools, EDD performs internal fraud mitigation efforts through the use of data cross-matching with the California Department of Corrections and Rehabilitation, Department of State Hospitals, and the Department of Juvenile Justice. The following sections describe these efforts in more detail.

5.1 Inter-Agency Cross-match and Internal Processes Fraud Mitigation

The following table details the potential fraud mitigated by EDD inter-agency cross-matches. At the time of this report's publication, 2024 data was only available through September 30, 2024.

Cases	Number of Claims	Fraud Mitigated
2024 Cross-Match Totals*	**UI: 525 DI: 17**	**UI: $2,360,179 DI: $33,159**

The following two tables provide details of potential fraud mitigated by utilizing internal-multiple claims per address and identity verification processes and procedures. EDD does this by comparing the addresses on the claimant's application. At the time of this report's publication, 2024 data was only available through September 30, 2024.

Multiple Claims per Address	Number of Claims	Fraud Mitigated
2024 Multiple Claims Totals	**UI Claims: 31,115 DI Claims: 4,357**	**UI: $ 153,486,483 DI: $2,494,460**

Internal Identity Verification	Number of Claims	Fraud Mitigated
2024 Totals	**UI Claims: 44,376 DI Claims: 25,482**	**UI: $ 149,545,333 DI: $63,385,810**

6 Public Awareness Campaigns and Collaboration with Law Enforcement

EDD regularly reviews and updates public-facing information related to fraud. The Department communicates with a high level of detail to the public, including non-claimants, claimants, employers, physicians/practitioners, and potential fraudsters at edd.ca.gov/FightFraud.

EDD's web page also includes a "How to Avoid Scams" section. Benefit programs are frequently susceptible to exploitation by fraudsters seeking to obtain benefits through the illicit use of individuals' personally identifiable information. EDD encourages individuals to report suspected fraud and provides four methods for contacting the Department. EDD also publishes a "What You Should Know About Unemployment Scammers" guide in 6 languages other than English including Armenian, Simplified Chinese, Traditional Chinese, Korean, Tagalog, and Vietnamese. The Department also regularly partners with media outlets to raise awareness of evolving tactics used by scammers.

EDD publicly provides fraud prevention statistics on investigations, arrests, and convictions for fraud on its Response to Fraud webpage. Further information regarding EDD's ongoing collaboration with law enforcement is contained in the Department's Annual Fraud Report.

7 Fraud Governance Group

EDD's Fraud Governance Group is a key component of the Department's successful fraud prevention efforts. The group effectively coordinates and guides various initiatives, such as identity verification, fraud detection, data sharing, public awareness, and law enforcement strategy. By providing a centralized forum for decision-making, coordination, and oversight, the Fraud Governance Group helps EDD effectively prevent and detect fraud, protect public funds, and maintain the integrity of its programs.

8 Summary

The fraud prevention tools, TR and ID.me, that were successfully implemented in 2020 and leveraged extensively to assist EDD in combating the unprecedented level of fraud attacks during the COVID-19 pandemic continue to be key in preventing fraud.

EDD's fraud prevention and detection tools assessment provide a critical lens through which EDD can continue to gauge the effectiveness of the technologies it employs to defeat benefit fraud and safeguard taxpayer funds while not unnecessarily burdening legitimate claimants. The transition to Socure in 2025 will further enhance EDD's fraud detection and prevention tools, while also improving the experience of EDD's customers. EDD continues to evaluate whether the right technologies are deployed in its layered, multi-component fraud prevention and detection technology stack and to identify where it needs to improve, potentially with different technologies or the reconfiguration of existing solutions.

STATE OF CALIFORNIA

LABOR & WORKFORCE DEVELOPMENT AGENCY

EMPLOYMENT DEVELOPMENT DEPARTMENT