Employment Development Department
State of California

Fraud Tools Assessment

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 EDD to provide a report to the California State Legislature on the effectiveness of the department's fraud prevention and detection tools annually beginning January 1, 2023.

In response to this requirement, this document offers the fraud tools assessment conducted by EDD for 2023. The core information covered in this report is substantially similar to the 2022 assessment prepared for the Legislature, while including notable updates related to the selection of a new identify proofing vendor and updated data documenting the impact of the EDD's fraud detection and prevention tools.

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 and outlines the point system that EDD utilizes to evaluate tool functionality and the effectiveness of the tool in achieving the intended business outcome. EDD appreciates the Legislature's discretion handling these sensitive matters and may provide additional details of the assessment in a private forum upon request.

2 Scope of Fraud Assessment Tool Review

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 adopts a layered, multi-component fraud prevention and detection technology solution, with the collective intent to safeguard taxpayer funds, while continuing to pay claimants timely. The scope of this tools assessment is focused on the effectiveness of the two primary fraud identification and detection tool vendors supporting the UI and SDI programs, specifically Thomson Reuters (TR) [Pondera and CLEAR platform] and ID.me, which are utilized to mitigate fraud.

This assessment evaluates how these fraud tools and services are currently used by EDD and the effectiveness of the tools to detect and/or prevent possible fraud schemes compared to industry best practices; it provides recommendations on how EDD can continually improve its fraud mitigation program. Also detailed is data pertaining to mitigated fraud as conducted through additional internal EDD processes involving cross-match verification with the California Department of Corrections and Rehabilitation (CDCR), Department of State Hospitals (DSH), and the Department of

Juvenile Justice (DJJ), as well as, multiple claims per address and identity verification procedures.

Fraud Prevention Tools in Scope

#	Solution Name	Description
1	**Thompson Reuters (TR)**	EDD currently uses TR as a fraud detection tool in conjunction with EDD's internal screening criteria. The following are TR services provided to EDD: • Fraud detection screening; • Business intelligence; and • Investigations management TR services are utilized to screen new UI and SDI customers for non-identity related fraud risk (e.g., mailing address, county and federal incarceration status). TR is also used to complement EDD's manual process to screen identity related fraud risk for paper and phone UI claim filers. For purposes of this assessment, the focus is on TR's fraud detection capabilities. TR was implemented in December 2020.
2	**ID.me**	EDD currently uses ID.me as an identity verification tool. It verifies identities of claimants who apply through the shared customer portal (SCP), which serves as the public facing portal for UI and SDI customers. In accordance with 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.

3 Tool Classification

The fraud prevention tools assessment specifies EDD's fraud prevention and detection solutions as falling into distinct categories. This categorization enables EDD to evaluate the efficacy of each solution against a predetermined set of respective features applicable to each tool category.

TR is classified as a **fraud detection tool**; it evaluates the probability that a claim is fraudulent using internal and third-party data sources. TR information is reviewed on the following parameters:

- Efficacy of existing fraud filters;
- Sources referenced;
- Potential gaps in capabilities that may require the development of new rules or features, and;
- Outputs generated by the tool.

ID.me is classified as an **identity verification tool** that authenticates a given person's identity via user-provided information, documents, and "selfie" images. 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. With the tool, many potential data points can be used to substantiate a claimant's identity. As an identity verification provider, ID.me is evaluated based on how it conforms to National Institute of Standards and Technology (NIST) Security Standards 800-63-3 [Identity Assurance Level 2] for Identity Verification. These security standards are designed to help ensure that only the right people have access to important information by verifying their identities.

4 Fraud Assessment – High Level Approach Background

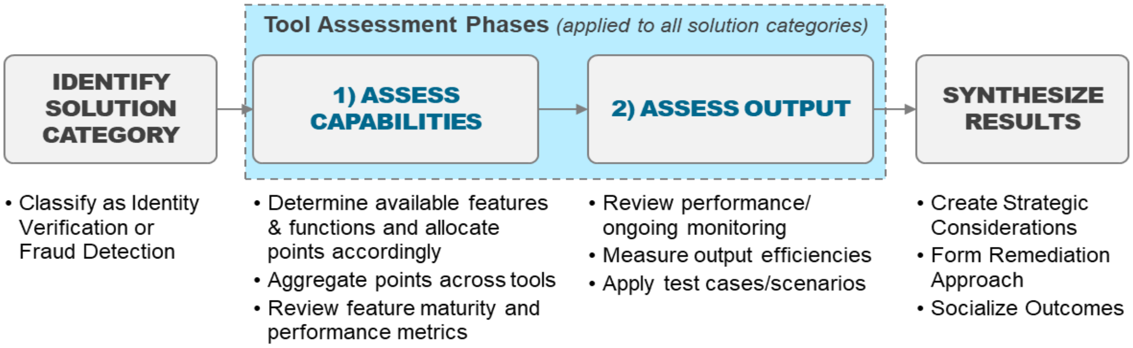
Starting in June 2021, EDD issued requests to its fraud tool partners, ID.me and TR, to provide access to information including artifacts, bespoke work products, and underlying EDD data as applicable, to enable the assessment of each of the fraud tools.

In response to the legislative updates related to Assembly Bill 56 (Chapter 510, Statutes of 2021), EDD aligned its assessment prioritizing compliance with NIST 800-63-3 for its identity verification tool, ID.me.

Below is a summary of the methods used to evaluate the fraud detection tool, TR, with the capabilities assessment approach described in further detail in Section 5 of this document.

To assess the effectiveness of its UI fraud prevention and detection tools, EDD follows a common and flexible methodology so that a diverse set of tools may be evaluated. Tools are classified into a common solution category (identity verification or fraud detection) to determine applicable use cases and appropriate assessment criteria. Next, tools undergo a two-phased assessment. This tool assessment process is visually depicted in Figure 1 on the next page:

Figure 1: High-level tool assessment approach


Tool Assessment Phases (applied to all solution categories)
IDENTIFY SOLUTION CATEGORY
1) ASSESS CAPABILITIES
2) ASSESS OUTPUT
SYNTHESIZE RESULTS

- Classify as Identity Verification or Fraud Detection

- Determine available features & functions and allocate points accordingly
- Aggregate points across tools
- Review feature maturity and performance metrics

- Review performance/ ongoing monitoring
- Measure output efficiencies
- Apply test cases/scenarios

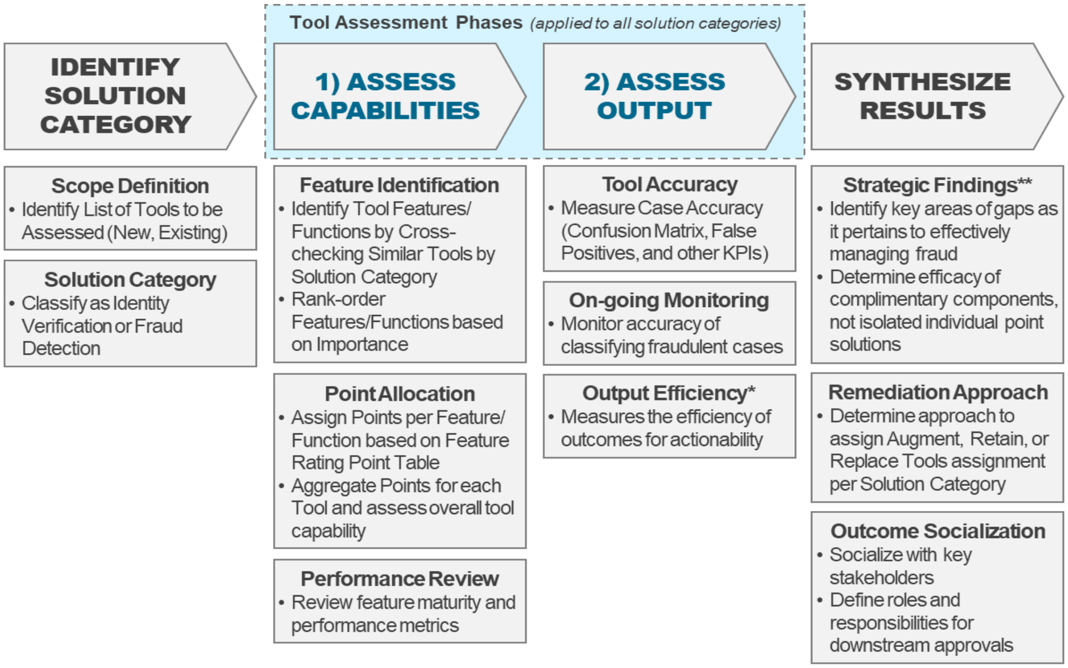
- Create Strategic Considerations
- Form Remediation Approach
- Socialize Outcomes

Phase one of the tool assessment process requires the features of the tool to be allocated points, and the tool be assessed for capabilities. During phase two, the tool undergoes output testing whereby various criteria, such as tool accuracy and ongoing monitoring, are applied and measured. Results are then synthesized and socialized in the form of strategic considerations to enhance EDD's fraud tools and approach to remediating identified gaps.

Initial pre-defined criteria have been developed to supplement each assessment phase. For example, phase one ("Assess Capabilities") utilizes representative features found among industry solutions to assist in identifying best-in-class functionalities EDD should consider.

On the following page is a diagram representing a detailed view of key activities across each phase of the approach (Figure 2) and an overview of the tool assessment steps (Figure 3).

Figure 2: Tool assessment approach detail



Tool Assessment Phases *(applied to all solution categories)*

IDENTIFY SOLUTION CATEGORY

Scope Definition
- Identify List of Tools to be Assessed (New, Existing)

Solution Category
- Classify as Identity Verification or Fraud Detection

1) ASSESS CAPABILITIES

Feature Identification
- Identify Tool Features/ Functions by Cross-checking Similar Tools by Solution Category
- Rank-order Features/Functions based on Importance

Point Allocation
- Assign Points per Feature/ Function based on Feature Rating Point Table
- Aggregate Points for each Tool and assess overall tool capability

Performance Review
- Review feature maturity and performance metrics

2) ASSESS OUTPUT

Tool Accuracy
- Measure Case Accuracy (Confusion Matrix, False Positives, and other KPIs)

On-going Monitoring
- Monitor accuracy of classifying fraudulent cases

Output Efficiency*
- Measures the efficiency of outcomes for actionability

SYNTHESIZE RESULTS

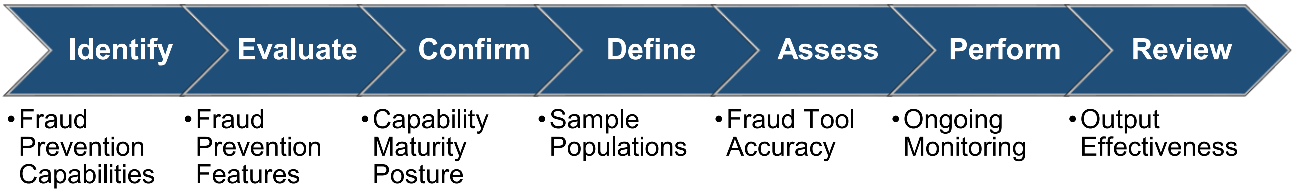
Strategic Findings**
- Identify key areas of gaps as it pertains to effectively managing fraud
- Determine efficacy of complimentary components, not isolated individual point solutions

Remediation Approach
- Determine approach to assign Augment, Retain, or Replace Tools assignment per Solution Category

Outcome Socialization
- Socialize with key stakeholders
- Define roles and responsibilities for downstream approvals

**output efficiency will be applied where applicable based on the nature of tool outputs*
***findings subject to discussions with vendors and negotiations, if any, for new technologies*

Figure 3: Tool assessment approach steps in summary



Identify
- Fraud Prevention Capabilities

Evaluate
- Fraud Prevention Features

Confirm
- Capability Maturity Posture

Define
- Sample Populations

Assess
- Fraud Tool Accuracy

Perform
- Ongoing Monitoring

Review
- Output Effectiveness

5 Assessment Observations – Capabilities and Outputs

EDD and Accenture evaluated the features and functionalities of each tool and the effectiveness of those capabilities when compared against EDD's final disposition of a claim. Capabilities and Output are used to assess the ability of the tools' effectiveness to identify and prevent potential fraud across EDD. To ensure robust and accurate findings from the tools assessment process, EDD has performed due diligence by working with the fraud detection/prevention vendors and requiring detailed review of the necessary information.

5.1 Capabilities Assessment Approach

Capability assessments were performed according to a tool's classification (identity verification or fraud protection). The purpose of this step is to qualitatively evaluate the existence of features and functions, examine the maturity of each capability, and quantitatively assign points for each feature according to a pre-determined scoring scale. In addition to the capabilities assessment approach, EDD also considered the effectiveness of TR's fraud prevention tool by assessing its performance in two key areas:

- Efficacy in fraud avoidance
- Alignment with industry standard baseline features for fraud detection

5.2 Output Assessment Approach

The next phase in the assessment analyzes a given tool's performance based on the accuracy of its results when evaluated against EDD's final disposition of a claim. The "confusion matrix"[*] is a common framework in data analytics and plays a significant role in describing the performance of a classification model, as in the case of the UI fraud detection tool, which is attempting to "classify," or distinguish between fraudulent and legitimate claims. Testing the tool's output provides the necessary data to complete a "confusion matrix."

5.3 Thomson Reuters (TR) – Status and Observations

In March 2021, EDD initiated information gathering for both a capabilities assessment and output evaluation of TR's fraud detection solution. From its interaction with TR, the department identified and documented requirements related to data, artifacts, and business rules needed to conduct its assessment. Much of the requested information and data were associated with bespoke work products defined by EDD with technical guidance from TR. In addition, EDD collected data that was made available by TR to secure information and the artifacts needed to perform and complete this assessment.

5.3.1 TR – Capabilities Assessment

EDD performed an assessment of TR defined features and functions for fraud detection tools from a list of recommended requirements for a fraud detection solution in 2022, which is being leveraged for this report. Each feature identified was reviewed and assigned a coverage rating based on its criticality, maturity, and availability within the tool. In addition, EDD performed the assessment outlined below of TR against a reference list of 8 industry defined features and functions for fraud detection tools. Our evaluation indicated that the TR tools provide these features and functions. See the table on the following page for a list and description of these features.

[*] A confusion matrix is a tabular summary of the number of correct and incorrect predictions made by a classifier.

Feature	Description	Met
Identity Verification Risk Scoring	Ability to risk score individuals identifying areas of risk such as shared values (home address, IP address, email address), deceased individuals, behavior pattern matching, and other anomalies. Results trigger alerts and populate claimant profiles.	Yes
Employer Validation	Ability to run existing employers against data sources to identify areas of risk. Results trigger alerts and populate the employer profiles.	Yes
Procedural Flagging	Results can trigger alerts and will be added to claimant and employer profiles.	Yes
Geospatial Analysis	Ability to geocode claimant and employer data for use in geospatial analysis to analyze relationships across participants and detect geographical anomalies in claim filings.	Yes
Street View	Provide street-level mapping to view claimant and employer locations.	Yes
Data Matching	Match data for claimants and employers against multiple lists used for fraud detection.	Yes
Scorecard	Scorecard provides EDD with ready access to claimants' associated risk score.	Yes
Fictitious Employer Schemes	Ability to allow users to view and compare behaviors of businesses and their claimants with aggregated patterns over time.	Yes

5.3.2 TR – Output Assessment

EDD's review of TR's performance as a part of its outputs assessment was conducted with data and documentation available on or before January 5, 2022. The 2020 historical and 2021 normalized data analysis enabled the department to evaluate how the tool uses input data, business rule logic, and associated rule codes to generate alerts. The review of TR's performance against two distinct claimant sample populations provided part of its output assessment of the TR solution.

The assessment conducted on TR Risk Categories ("filters") indicates that the TR tool did address the criteria that were specific to EDD's needs during the pandemic that were not being met by our other processes. The TR tool remains a valuable resource that plays an important role in EDD's overall fraud prevention strategy.

5.3.3 TR – Mitigated Fraud

The table below represents the number of claims and estimated amount of fraud mitigated due to the use of the TR tool. At the time of this report's publication, 2023 data was only available through November 30, 2023, and only includes UI claims. DI claim data will be reported beginning in the 2024 report year.

TR – Calendar Year	UI Fraud Claims Prevented	UI Fraud Mitigated
2023 YTD Total	**21,837**	**$62,288,834**

5.3.4 TR – Next Steps

EDD will continue to identify any and all constraints and limitations within the TR provided information regarding its algorithms and business rules documentation, the output assessment, and requirements. EDD will continue to review data, data mapping, visibility into rules logic, feature/functionality and documentation, and the root causes of any discrepancies, to refine techniques to optimize the filters.

In January 2022, EDD worked with TR to update the Result Based Rule Calibration, to improve the fraud detection processes; there are recurring checkpoints to calibrate rules based on fraud and non-fraud determinations and trends. The Results Based Rule Calibration ensures EDD's fraud filters align with evolving behaviors of legitimate customers and fraudsters while maintaining the effectiveness of the filters in preventing fraud. EDD also continues collaborating with TR to configure the solution to meet EDD's requirements.

5.4 ID.me – Status and Observations

In December 2021, EDD initiated the capabilities aspect of the tools assessment for ID.me. In September 2022, the Department modified its assessment approach of the Identity Verification tool to include an assessment against the established NIST 800-63a standard for Identity Verification. EDD had an independent assessment of ID.me conducted by a Kantara-Accredited Assessor between January 2023 and March 2023. The Kantara-Accredited Assessor confirmed ID.me meets the requirements for a full credential service provider in conformity with NIST SP 800-63 rev.2 at IAL2/AAL2.

5.4.1 ID.me – Capabilities Assessment

Prior to adopting ID.me, EDD initiated its assessment of ID.me against a reference list of defined features and functions for identity verification tools based on an assessment vendor recommendation. As part of the Governor's Strike Team Report dated September 16, 2020, EDD adopted ID.me as a solution due to its capability of identity proofing to NIST Identity Assurance Level 2 & Authorization Assurance Level 2 11 (IAL2/AAL2), as defined in the NIST special publication 800-63-3, which provides guidelines on implementing digital identity services. NIST Identity Assurance Level 2 is designed to help ensure that only the right people have access to important information by verifying their identities. In following the NIST standard, processes and procedures are put in place that only allow authorized people to access important or confidential information using methods such as passwords or biometric identification.

This helps protect against fraud and unauthorized access to sensitive information. Due to the alignment of ID.me to NIST Identity Assurance Level 2, EDD was able to meet its requirements for the features required for identity verification tools by adopting ID.me as a tool.

5.4.2 ID.me – Output Assessment

EDD output analysis pertaining to ID.me's performance is continuously reviewed. Given the alignment of ID.me to the Identity Assurance Level 2 & Authorization Level 2 11 (IAL2/AAL2) (as defined in NIST special publication 800-63-3), EDD assessment of ID.me's secure identity verification process is satisfactory due to its compliance with NIST Identity Assurance Level 2.

5.4.3 ID.me – Mitigated Fraud

Data collected from January 1, 2023, through November 30, 2023, has been broken down separately for UI claimants, DI claimants, and DI medical providers into three separate tables, which can be viewed on the subsequent page of the report.

Each of the three tables provides a total for the number of claimants who started the verification process. These claimant numbers are then further broken down into four separate categories that describe the outcome of the verification process—claimants who abandoned the verification process, claimants currently going through the process on November 30, 2023, unsuccessful claimants, and verified claimants. The data is further tabulated based on whether claimants attempted to use a trusted referee (a trained identity specialist employed by ID.me who conducts live virtual meeting with claimants to confirm their identities) or verified their identity through self-service methods.

ID.me has been an important component of EDD's fraud prevention toolbox. From January 1, 2023, through November 30, 2023, the ID.me platform prevented 78,247 potentially fraudulent UI claims from being filed, 7,813 potentially fraudulent DI claims from being filed, and 344 potentially fraudulent DI medical provider certifications from being filed.

January 1, 2023 – November 30, 2023: UI Claimants
Started Verification: 692, 944
Abandoned[†]: 50,678 (-7.3%)

	Attempted Trusted Referee[‡]	Did Not Attempt Trusted Referee	Self-Service	Trusted Referee	Total
Processing[§]	865 (-27.5%)	2,281 (-72.5%)	N/A	N/A	3,146 (-0.5%)
Unsuccessful	37,271 (-23.1%)	123,773 (-76.9%)	N/A	N/A	161,044 (-23.2%)
Verified	N/A	N/A	389,348 (-81.4%)	88,728 (-18.6%)	478,076 (-69.0%)

Estimated Fraud Prevented: 78,247 Individuals

January 1, 2023 – November 30, 2023: SDI Claimants
Started Verification: 665,572
Abandoned: 32,329 (-4.9%)

	Attempted Trusted Referee	Did Not Attempt Trusted Referee	Self-Service	Trusted Referee	Total
Processing	409 (-21.6%)	1,486 (-78.4%)	N/A	N/A	1,895 (-0.3%)
Unsuccessful	16,946 (-17.7%)	78,911 (-82.3%)	N/A	N/A	95,857 (-14.4%)
Verified	N/A	N/A	462,520 (-86.4%)	72,971 (-13.6%)	535,491 (-80.5%)

Estimated Fraud Prevented: 7,813 Individuals

January 1, 2023 – November 30, 2023: Medical Providers
Started Verification: 10,986
Abandoned: 1,152 (-10.5%)

	Attempted Trusted Referee	Did Not Attempt Trusted Referee	Self-Service	Trusted Referee	Total
Processing	6 (-11.3%)	47 (-88.7%)	N/A	N/A	53 (-0.5%)
Unsuccessful	279 (-9.0%)	2,824 (-91.0%)	N/A	N/A	3,103 (-28.2%)
Verified	N/A	N/A	6,045 (-90.5%)	633 (-9.5%)	6,678 (-60.8%)

Estimated Fraud Prevented: 344 Individuals

The estimated fraudulent users that ID.me is blocking from completing identity verification is calculated based on ID.me Security and Data Analytics teams' monitoring of social engineering, synthetic identity theft, and other fraudulent activity

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

[‡] A trusted referee is a trained identity specialist employed by ID.me who conducts live virtual interviews with claimants to confirm their identities.

[§] Represents the claims actively in process on November 30, 2023, when this data was snapshotted.

across state/federal partners including component vendor fraud flags, duplicate personal identifiable information, and supervised attempts.

5.4.4 ID.me – Additional Assessment Information

EDD also evaluated the following additional factors for ID.me that are important for any identity verification toolset that is used with our fraud efforts.

Area	Finding	Follow Up Action
Accessibility	When using ID.me, if someone is unable to verify their identity through the automated process, they must go through a live virtual interview with ID.me via a trusted referee. This requires a strong enough broadband internet connection to transmit live video. There are areas in California that do not have strong broadband access.	Identify alternative solutions that can provide additional rapid verification using alternative technologies that do not rely on virtual interviews.
Data retention	Identity data is stored externally by ID.me and EDD does not have access to the data. Selfie images and associated biometric data are deleted after 24 hours.	Identify alternative solutions that provide data retention under EDD's control. However, EDD would not store any biometric data.
Processing Time	Current wait times for ID.me supervised chats have been reduced to three minutes from much longer wait times that existed in 2022. EDD will continue to work with ID.me on solutions to keep wait times low for EDD customers and identify alternative solutions that can provide additional rapid verification using alternative technologies, as needed.	N/A
Verification Processing	Upfront fraud detection via IP addresses or the option to call in an Application Program Interface in a batch type format (i.e., push to have every transaction vetted in real time, options to do batch vetting as well, etc.) is currently being leveraged.	Identify alternative solutions that can provide additional upfront verification using alternative technologies such as real-time IP address and device risk checks.

5.4.5 ID.me – Next Steps

EDD requested and received from ID.me the NIST 800-63-3 IAL2 & AAL2 Annual Conformity Review on June 14, 2023.
Market research was conducted in 2023 on four identity verification vendors and an alternative vendor was selected. A RFP (request for proposal) was initiated in October 2023. Adopting a new identity verification service provider will necessitate continuous monitoring to ensure fraud detection capabilities continue with service level parity. In December of 2023, EDD finalized the procurement process for Socure, which will provide claimants with the opportunity to verify their identity without uploading documents. EDD expects to deploy their technology in 2024.

The current contract with ID.me is in place through June 2024 but will be incrementally extended as needed until the alternative vendor has fully implemented its identity verification platform.

5.5 Internal Processes and Cross Matches

In addition to the TR and ID.me tools, EDD performs internal fraud mitigation efforts through the use of cross-matching against data sharing with the California Department of Corrections and Rehabilitation (CDCR), Department of State Hospitals (DSH), and the Department of Juvenile Justice (DJJ).

5.5.1 Internal Processes and Cross-match Fraud Mitigation

The following table details the potential fraud mitigated by EDD using cross-matches with the CDCR, DSH, and the DJJ. At the time of this report's publication, 2023 data was only available through November 30, 2023.

Cases	Number of UI Claims	Fraud Mitigated
2023 Cross-Match Totals**	**254**	**$ 1,206,909**

** EDD established data sharing with the CDCR in May 2023 regarding DI claims. Fraud data for DI claims will be reported in 2024.

The following two tables provide details of potential fraud mitigated by utilizing internal multiple claims per address and identity verification processes and procedures. At the time of this report's publication, 2023 data was only available through November 30, 2023.

Multiple Claims per Address	Number of Claims	Fraud Mitigated
2023 Multiple Claims Totals	**UI Claims: 23,739** **DI Claims: 4,246**	**UI: $ 72,257,815** **DI: $ 6,467,170**

Internal Identity Verification	Number of Claims	Fraud Mitigated
2023 Totals	**UI Claims: 67,013** **DI Claims: 11,611**	**UI: $ 292,227,872** **DI: $ 326,692,895**

5.5.2 National Association of State Workforce Agencies Integrity Data Hub

The National Association of State Workforce Agencies (NASWA) Integrity Data Hub (IDH) is a multistate data system with advanced data cross-matching and analysis capability that detects and prevents UI fraud and improper payments. California is one of the participating states via EDD. The NASWA IDH was implemented at EDD on June 28th, 2023. Currently, EDD shares UI new claim data and provides updates to the NASWA IDH daily. Result files have been sent back to EDD as well for review and investigation. EDD is currently reviewing the information from NASWA IDH and defining the business requirements for the next phase of the NASWA IDH project.

6 Findings and Recommendations

EDD discovered areas for continual improvement to address items that need additional attention to avoid increased risk, assist with decision making, and/or direct activities to combat the continually evolving fraud threat landscape. Every tool used in combating fraud will be evaluated annually to ensure that EDD is continually leveraging the best and most effective detection and prevention tools.

Findings	Follow Up Actions
NIST provides standard frameworks which allow for security and fraud controls to be evaluated during the vendor assessment and selection process.	Continue to apply NIST standards to assess the effectiveness of fraud tools implementation when possible.
The fraud landscape is continually evolving, causing tool vendors to change	Continue to recalibrate baselines based on the continuously evolving fraud schemes. Evaluate vendors that can be leveraged to combat fraud with readily

their systems, which often leads to inconsistent baselines.	available Key Performance Indicators (metrics to determine the baseline effectiveness of each tool) or standards-based alignment.
EDD's legacy systems, environments, processes, and data repositories limit the types of fraud tools that could be leveraged to combat fraud in a streamlined manner.	Modernize, standardize, and implement a new technology environment during the EDDNext project to enable expanded agile, scalable, secure, and equitable fraud detection tools adoption.

7 Summary

The fraud prevention tools TR and ID.me were quickly and successfully implemented in 2020 and leveraged extensively to assist EDD in combating the unprecedented level of fraud attacks during the COVID-19 pandemic. EDD implemented ID.me as a real time service for online users, including UI claimants, and most recently, DI claimants and medical providers that certify those claims.

To supplement the use of ID.me, EDD also partnered with TR to provide checks for claimants' identity information that file a claim by phone, paper (non-online scenarios) – as well as for non-identity fraud scenarios (e.g., mailing address fraud, county and other U.S. states incarceration status, etc.). Implementing these fraud prevention tools during the pandemic strengthened EDD's ability to detect and prevent fraud.

The EDD fraud prevention and detection tools assessment provides a critical lens through which EDD can continue to gauge the effectiveness of the technologies it employs to defeat benefit fraud and to safeguard taxpayer funds while not unnecessarily burdening legitimate claimants. In doing so, EDD will continue 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.

Elements of the EDD assessment will also serve as reusable components to allow for the ongoing monitoring of existing solutions and as a repeatable framework to assess and adjust the fraud prevention and detection technology stack as threats from fraudsters inevitably adapt to existing defenses. Most importantly, this ongoing and repeatable process will reinforce EDD's culture of fraud awareness and action, mitigating future risk to the state of California's taxpayer funds and claimants alike.

This assessment has identified key areas of improvement that EDD has continued to enhance. As directed by EDD, TR and ID.me continue to adhere to requested modifications to remain at a level of readiness to combat fraud in the constantly evolving fraud landscape while also respecting and safeguarding our clients' information. The transition to Socure in 2024 will further enhance EDD's fraud detection and prevention tools, while also improving the experience of EDD's customers. This report is a living document that the Legislature can reference in our joint effort to reduce occurrences of fraud while serving our constituents in a secure, equitable, and efficient manner.

Employment
Development
Department
State of California

STATE OF CALIFORNIA

LABOR & WORKFORCE DEVELOPMENT AGENCY

EMPLOYMENT DEVELOPMENT DEPARTMENT