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 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. The Department has utilized supporting assistance provided by IT consulting firm Accenture by way of its tools review and analysis.

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 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 unemployment insurance (UI) program, specifically Thomson Reuters [Pondera and CLEAR platform] and ID.me, which are utilized to mitigate vulnerabilities exploitable by threat agents. 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 and 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.

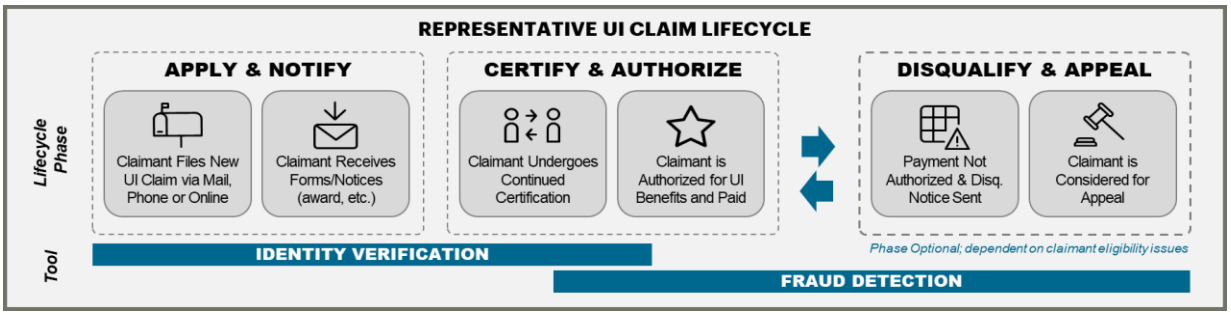
Fraud Prevention Tools in Scope

#	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 offerings to EDD: • Fraud detection screening; • Business intelligence; and • Investigations management TR services are utilized to screen new UI 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 the purpose 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 authenticates identities of claimants who apply using the unemployment insurance online (UIO) application portal. 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.

Figure 1: UI Claim Lifecycle and Solution Category Applicability



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 is reviewed on the following parameters:

- Efficacy of existing business rules;
- 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. Claimants may also opt out of the "selfie" image process and not share their biometric information. 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 800-66 [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

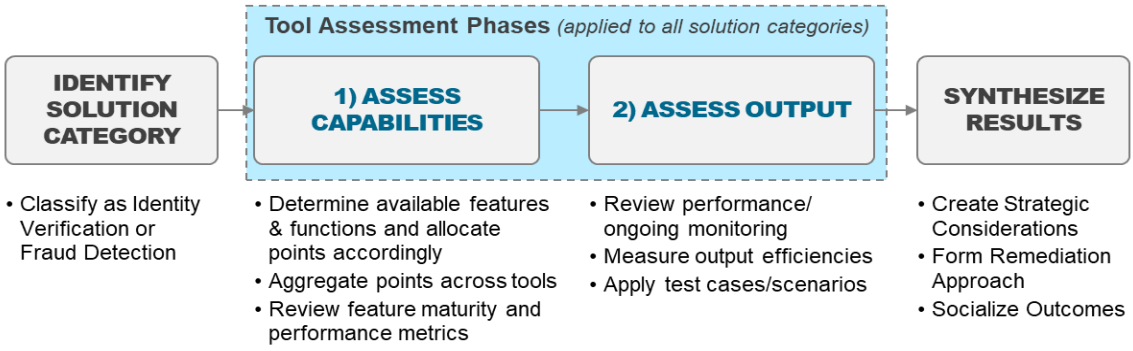
Starting in June 2021, EDD issued requests to its fraud tool partners, ID.me and Thomson Reuters, to provide access to information including artifacts, bespoke work products, and underlying EDD data as applicable, to enable the assessment of each of the fraud tools.

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 for its identity-related fraud prevention 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 2 below:

Figure 1: High-level tool assessment approach

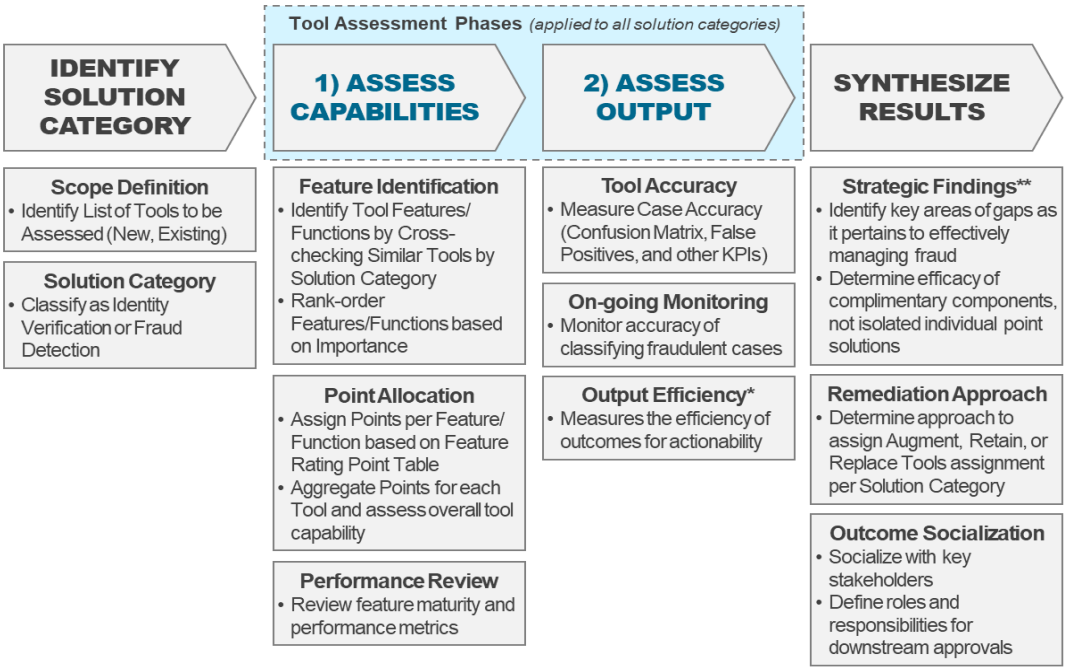


Phase one of the tool assessment process requires the features of the tool to be allocated points, and the tool be assessed for capabilities. During phase two, the tool undergoes output testing whereby various criteria, such as tool accuracy and ongoing monitoring, are applied and measured. Results are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

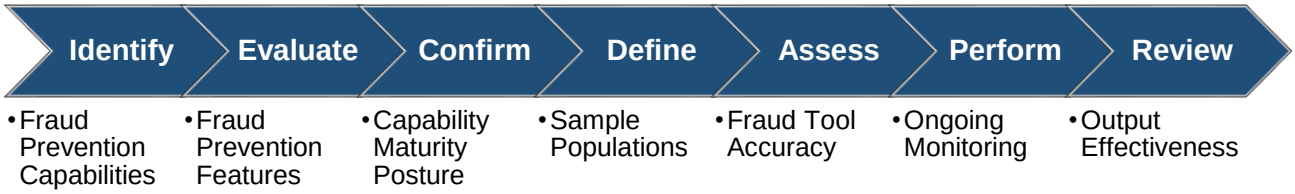
The following page contains a diagram representing a detailed view of key activities across each phase of the approach (Figure 3) and an overview of the tool assessment steps (Figure 4).

Figure 2: Tool assessment approach detail



**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 4: Tool assessment approach steps in summary



5 Assessment Observations – Capabilities and Outputs

EDD directed Accenture to evaluate 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 formally requesting the necessary information from third party software vendors.

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 Pondera'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 will provide necessary data to complete a "confusion matrix."[1]

5.3 Thomson Reuters (TR) Pondera – 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 Pondera – 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. Each feature identified was reviewed and assigned a coverage rating based on its criticality, maturity, and availability within the tool.

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

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.

Feature	Description	Met
Claimant Validation	Ability to run current claimants through system to identify areas of risk such as shared values (such as home address, IP address, e-mail address), deceased participants, behavioral pattern matching, and other anomalies. Results trigger alerts and populate the 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 on the Dashboard 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.	Yes
Street View	Provide street-level mapping to view claimant and employer locations from within the dashboard	Yes
Data Matching	Match data for claimants and employers against multiple lists used for fraud detection.	Yes
Scorecard	Scorecard provides users with ready access to claimants and their 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 Pondera – Output Assessment

EDD's review of TR Pondera'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 Pondera's performance against two distinct claimant sample populations provided part of its output assessment of the TR Pondera solution.

The assessment conducted on TR Risk Categories ("filters") indicates that the TR Pondera 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 Pondera – Mitigated Fraud

The table below represents the number of claims and estimated amount of fraud mitigated due to the use of the TR tool. In calendar years 2020 and 2021, a significant increase in unemployment insurance claims due to the COVID-19 pandemic impacted the number of fraud

claims prevented and the amount of fraud loses mitigated. Calendar year 2022 represents a more typical year.

TR - Calendar Year	Fraud Claims Prevented	Fraud Mitigated
2020 Total	703,378	$ 6,109,869,842
2021 Total	247,220	$ 4,379,141,875
2022 Total	50,725	$ 125,787,258

5.3.4 TR Pondera – Next Steps

EDD will continue to identify any and all constraints and limitations within the TR Pondera 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, to review root causes of any discrepancies, and techniques to optimize the filters.

In January 2022, EDD worked with TR to update two primary areas, Binary Alert Enhancement and Result Based Rule Calibration, to improve the fraud detection processes. The Results Based Rule Calibration ensures fewer legitimate customers are improperly impacted by the alert while maintaining the effectiveness of the alert in preventing fraud. EDD also continues collaborating with TR to configure the solution to meet EDD's requirements. While some information remains proprietary, EDD will request changes to terms and conditions to gain full access to items needed for evaluation purposes, including information held by third party.

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. The approach was modified due to the assessment vendor indicating that the information obtained from the tool vendor was insufficient to make a full assessment.

5.4.1 ID.me – Capabilities Assessment

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 Governors 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 remains in progress. 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

The table below gives figures for the total number of individuals who interfaced with the ID.me platform, the number of individuals who abandoned the ID.me process, those who were unsuccessful with verification, and those who successfully completed their verification from October 1, 2020 through December 31, 2022. Unsuccessful verification and completed verification figures are further broken down based on whether the individual utilized a trusted referee, a trained identity specialist employed by ID.me to prove the individual's identity. The use of the ID.me platform allowed for the prevention of approximately 2,640,375 potentially fraudulent claims from being filed.

Number of Individuals - 7,819,761*				
Abandoned Verification[2]	**Unsuccessful Verification**		**Completed and Verified**	
1,097,133	2,624,336		4,098,292	
	Attempted Trusted Referee	Did Not Attempt Trusted Referee	Attempted Trusted Referee	Did Not Attempt Trusted Referee
	924,628	1,699,708	3,361,725	736,567
14.0%	35.20%	64.80%	82.0%	18.0%
Estimated Fraud Prevented: 2,638,764 Individuals				

* Data cited in table was provided by ID.me.

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

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

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.
Processing Time	Wait times for ID.me supervised chats from January - March 2022 is 75.6 minutes as last reported by ID.me.	Current wait times for ID.me supervised chats have been reduced to 3 minutes. 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.
Verification Processing	Upfront fraud detection via IP addressing 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.

5.4.5 ID.me – Next Steps

EDD worked with ID.me over the past year to discuss capabilities, data availability, process documentation, model control, and overall governance. The department will proceed with the outputs analysis reviewing any additional features ID.me makes to its solution (including and not

limited to changes to user privacy, model changes, and any additional functionality) as appropriate data and documentation are made available. While some information remains proprietary, EDD will request changes to contract terms and conditions to gain full access to items needed for evaluation purposes.

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

Data from calendar years 2020 and 2021 displayed in the tables below was impacted by the significant increase in claims made due to the COVID-19 pandemic.

The following table details the potential fraud mitigated by EDD using cross-matches with the CDCR, DSH, and the DJJ.

Cases	Number of Claims	Fraud Mitigated
2020 Cross-Match Totals	**793**	**$ 4,014,690**
2021 Cross-Match Totals	**655**	**$ 5,357,534**
2022 Cross-Match Totals	**429**	**$ 2,288,439**

The following two tables provide details of potential fraud mitigated by utilizing internal multiple claims per address and identity verification processes and procedures.

Multiple Claims per Address	Number of Claims	Fraud Mitigated
2021 Multiple Claims Totals	**423,604**	**$ 7,990,074,209**
2022 Multiple Claims Totals	**30,857**	**$ 188,837,896**

Internal Identity Verification	Number of Claims	Fraud Mitigated
2020 Total	**2,170,418**	**$ 21,106,956,797**
2021 Total	**237,392**	**$ 2,422,323,056**
2022 Total	**90,316**	**$ 623,812,222**

5.5.2 Fraud Mitigated - All EDD Tools

The table below represents the cumulative potential fraud mitigating by EDD inclusive of TR, ID.me, internal controls and processes are listed below for the respective calendar years. Data

from calendar years 2020 and 2021 displayed in the table below was impacted by the significant increase in claims made due to the COVID-19 pandemic.

Calendar Years	Number of Claims	Total Fraud Mitigated
2020 Totals	**2,874,589**	**$ 27,220,841,329**
2021 Totals	**908,871**	**$ 14,796,896,674**
2022 Totals	**172,327**	**$ 940,725,815**

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 their systems, which often leads to inconsistent baselines.	Continue to recalibrate baselines based on the continuously evolving fraud schemes. Evaluate vendors that can be leveraged to combat fraud with readily 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. The EDD team implemented ID.me as a real time service for online users (i.e., for both unemployment insurance claimants, and most recently, disability insurance claimants and medical providers that certify those claims).

To supplement the use of ID.me, the EDD team 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 states incarceration status, etc.). Implementing these fraud prevention tools during the pandemic provided EDD relief and an improved fraud prevention and detection posture.

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 unemployment insurance fraud and to safeguard taxpayer funds while not unnecessarily burdening the distribution of legitimate claims. In doing so, EDD will continue to understand where the right technologies are within its layered, multi-component fraud prevention and detection technology stack and 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. The execution of this assessment will require support from the legislature to enable additional effort-sizing and attendant resources, which EDD would also have to accommodate as part of its budget.

This assessment has identified key areas of improvement that EDD has continued to enhance. As directed by EDD, both tool vendors 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. 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.

Gavin Newsom
Governor
STATE OF CALIFORNIA

Stewart Knox
Secretary
LABOR & WORKFORCE DEVELOPMENT AGENCY

Nancy Farias
Director
EMPLOYMENT DEVELOPMENT DEPARTMENT