Stage 1 Business Analysis

California Department of Technology, SIMM 19A.3 (Ver. 3.0.8, 02/01/2022)

1.1   General Information

1. **Agency or State entity Name: 7730 - Franchise Tax Board**

2. **Proposal Name and Acronym: Fraud, Analysis & Detection Solution Revise (FADSR)**

3. **Proposal Description: (Provide a brief description of your proposal in 500 characters or less.)**

The Franchise Tax Board (FTB) proposes to improve fraud detection capability. The solution will be designed to minimize the risk of the loss of general fund revenue to the state resulting from the issuance of erroneous tax refunds.

FTB strives to serve taxpayers by continually improving the quality of products and services and performing in a manner which secures the highest degree of taxpayer confidence with integrity, efficiency, and fairness.

This effort will help safeguard FTB's ability to protect its taxpayers and secure the state's general fund from refund fraud, which in turn funds services important to all Californians.

4. **Proposed Project Execution Start Date: 7/1/2026**

5. **S1BA Version Number: Version 1**

1.2   Submittal Information

1. **Contact Information**

    Contact Name: Christina Casale

    Contact Email: Christina.Casale@ftb.ca.gov

    Contact Phone: 916.845.4116

2. **Submission Type: New Submission**

    If Withdraw, select Reason: Choose an item.

If Other, specify reason here: Click or tap here to enter text.

Sections Changed, if this is a Submission Update: (List all sections changed.)

Click or tap here to enter text.

Summary of Changes: (Summarize updates made.)

Click or tap here to enter text.

3. Attach **Project Approval Executive Transmittal** to your email submission.

4. Attach **Stage 1 Project Reportability Assessment** to your email submission.

1.3   Business Sponsorship

1. **Executive Champion (Sponsor)**

   Title: C.E.A.

   Name: Roger Lackey

   Business Program Area: Filing Division-Fraud, Analysis & Detection Section

   Title: C.I.O.

   Name: Nadean Shavor

   Business Program Area: Technology Services Division

   Title: C.E.A.

   Name: Jeanne Harriman

   Business Program Area: Finance & Executive Services Division

2. **Business Owner**

   Title: C.E.A.

   Name: Scott Reid

   Business Program Area: Fraud, Analysis & Detection Section

   Title: Administrator IV

   Name: Cherrie Hayes

   Business Program Area: Fraud, Analysis & Detection Section

   Title: Administrator II

   Name: Calvin Brown

   Business Program Area: Fraud, Analysis & Detection Section

1.4   Stakeholder Assessment

The Stakeholder Assessment is designed to give the project team an overview of communication channels that the state entity needs to manage throughout the project. More stakeholders may result in increased complexity to a project.

1. **Indicate which of the following are interested in this proposal and/or the outcome of the project. (Select 'Yes' or 'No' for each.)**

    State Entity Only: Yes

    Other Departments/State Entities: No

    Public: No

    Federal Entities: No

    Governor's Office: No

    Legislature: No

    Media: No

    Local Entities: No

    Special Interest Groups: No

    Other: No

2. **Describe how each group marked 'Yes' will be involved in the planning process.**

    State Entity will be following the project for effectiveness and compliance with current state laws and regulations.

1.5   Business Program

3. **Business Program Name:** Fraud, Analysis and Detection Section

4. **Program Background and Context:** (Provide a brief overview of the entity's business program(s) current operations.)

    The Fraud, Analysis & Detection Solution Revise (FADSR) uses innovative selection methods and analytics to detect and prevent fraudulent claims and discover taxpayers who file false claims, + underreport their taxes, or attempt identity theft. We work as a department to provide professional, accurate, and timely service to our internal and external customers. Services provided include refund verification, identity theft detection and prevention, withholding fraud detection and prevention, and Earned Income Tax Credit validation.

    The FADSR Fraud Analysis team reviews tax return information and uses statistical data models in conjunction with expert modeling to identify new fraud patterns that are worked by FADSR technicians. The Identity Theft team works to reduce the instances of fraudulent

refunds issued to imposters using someone else's identity to file a fictitious tax return to request a refund that is not due to them. In addition, FADSR also identifies and stops wage withholding refund fraud by reviewing fraudulent W2s as well as performing modeling and analysis.

5. **How will this proposed project impact the product or services supported by the state entity?**

This project will help ensure FTB can continue to keep up to date with protectionary measures to reduce erroneous refunds. Specifically, it will allow FTB to:

- Evolve its fraud detection technology capabilities to ensure fraud is detected and prevented timely.

- Improve the ability to detect and prevent revenue losses to the state's general fund due to improper payments and fraudulent refunds being issued.

- Reduce processing timeframes for refunds.

- Support proper enforcement actions and ensure compliance activities are directed toward the correct individuals.

- Allow for faster implementation of technology solutions to address evolving fraud techniques.

- Improve data and process management for future filing seasons to impact fewer real taxpayers.

1.6 Project Justification

1. **Strategic Business Alignment**

   Enterprise Architect

   Title: Information Technology Manager II

   Name: Jason Hallford

   Strategic Plan Last Updated? 1/1/2021

   Strategic Business Goal: Effective Compliance

   Alignment: Fairly administer the law to ensure taxpayers file and pay the correct amount.

   2.3 Improve case selection and timeliness in all compliance programs.

   Enhancing FTB IT infrastructure will improve the use of large data sets to increase accuracy in the detection of fraudulent activity and improve the selection rates of possible fraudulent tax filings.

   Strategic Business Goal: Operational Excellence

Alignment: Optimize our processes, products, services, and resources to better serve our internal and external customers.

4.4 Mitigate emerging and evolving threats to manage risks and protect customer privacy and security.

The enhancements to the fraud process through the improvements of FTBs IT infrastructure will allow for increased detection and faster response times to new and evolving threats by allowing faster access to new data and improving existing functions including updates to data models to meet the more sophisticated threats allowing FTB to be proactive in protecting the taxpayer's data and general fund from losses.

Mandate(s): None

Bill Number/Code, if applicable: Click or tap here to enter text.

Add the Bill language that includes system-relevant requirements:

Click or tap here to enter text.

2. **Business Driver(s)**

Financial Benefit: Yes

Increased Revenue: No

Cost Savings: No

Cost Avoidance: Yes

Cost Recovery: No

Will the state incur a financial penalty or sanction if this proposal is not implemented? No

> If the answer to the above question is "Yes," please explain:
>
> Click or tap here to enter text.

Improvement

Better Services to the People of California: Yes

Efficiencies to Program Operations: Yes

Improved Equity, Diversity, and/or Inclusivity: No

Improved Health and/or Human Safety: No

Improved Information Security: Yes

Improved Business Continuity: Yes

Improved Technology Recovery: Yes

Technology Refresh: No

Technology End of Life: No

1.7   Business Outcomes Desired

Executive Summary of the Business Problem or Opportunity:

To ensure long term success of a fraud prevention program it is crucial in today's rapidly advancing technology to invest in new protectionary methods. As fraud tactics become increasingly sophisticated, organizations must stay ahead by regularly enhancing its strategies to protect sensitive information as well as financial assets. FTB works to not only safeguard against potential losses, but also build and maintain public trust. By integrating new tools, training and best practices FTB can effectively maintain its high standards of effective risk mitigation, responding to emerging threats, and maintain a resilient defense against future fraud attempts. To do so FADSR is requesting to update its current processes to bring in new tools, data and processes to be able to rapidly deploy new technologies, to combat new and emerging fraud threats.

We have seen massive increases in criminal syndicates, both foreign and domestic, that are filing fraudulent returns for refunds. These new cyber syndicates are highly organized, highly sophisticated and well-funded. We have seen over the past few years multiple government agencies both federal and state have reported losses. A recent report has shown a state department lost an estimated $55 billion due to fraud during the pandemic years. Another report showed the IRS losing $18.2 billion in improper payments in (2022-GAO-23-106285). FTB is working to maintain the high standard of success we have achieved in the last decade, but the threat scape is ever evolving as we have detected in the last year a 200% increase in in data breaches along with a 700% increase in erroneous payments stopped. To quantify the increase in risk and attempts from 2017-2020 the average amount of improper payments per year was approximately $150 million dollars saved. However, in the last three years the attempts have skyrocketed to over $1 billion dollars prevented each year. If this project were to prevent just one scheme like the magnitude illustrated in the examples above, the Return on Investment (ROI) would be $300 to $1 if not higher.

Objective ID: 1.0

Objective: Modernize FTB's internal data architecture to accelerate the availability of additional key data elements to improve the speed and effectiveness of fraud detection and prevention processes.

Metric: Increase the data frequency of additional key data elements to support fraud detection and prevention processes.

Baseline: Current data frequency of some data elements is on average 7 days.

Target Result: Upon implementation the data frequency of some data elements would be multiple times per day.

Objective ID: 2.0

Objective: Upon implementation confirm the developed interface supports on demand queries, reports, expert modeling, and anomaly detection workloads using data available to the department.

Metric: Confirm successful implementation of the functional data query and expert modeling interface developed by the project.

Baseline: Manual process to generate data queries.

Target Result: Implementation of a functional on demand data query, reporting and expert modeling tool that interfaces with data elements available to the department.

Objective ID: 3.0

Objective: Enhance fraud and identity theft detection capabilities to improve the quality of the fraud candidate pool and minimize FADSR taxpayer contact by achieving a ten percent reduction in the selection rate of tax returns requiring manual intervention for review.

Metric: Percentage reduction of possible fraud tax returns/cases selected for review.

Baseline: Each year, FADSR selects a portion of all filed tax returns. Of those selected for analysis, an average of 40% are selected for manual intervention.

Target Result: Of those selected for analysis, an average of 30% would be selected for manual intervention.

1.8 Project Management

1. **Project Management Risk Score: 0.6**

Project Management Risk Assessment Template FADS Revise

2. **Project Approval Lifecycle Completion and Project Execution Capacity Assessment**

Does the proposal development or project execution anticipate sharing resources (state staff, vendors, consultants, or financial) with other priorities within the Agency/state entity (projects, PALs, or programmatic/technology workload)?

Answer: Yes

Does the Agency/state entity anticipate this proposal will result in the creation of new business processes or changes to existing business processes?

Answer (No, New, Existing, or Both)**:** Both New and Existing Processes

1.9   Initial Complexity Assessment

1. **Business Complexity Score:** 1.9

   SIMM 45 Appendix C-Complexity Assessment

2. **Noncompliance Issues:** (Indicate if your current operations include noncompliance issues and provide a narrative explaining how the business process is noncompliant.)

   Programmatic regulations: No

   HIPAA/CIIS/FTI/PII/PCI: No

   Security: No

   ADA: No

   Other: No

   Not Applicable: No

   Noncompliance Description: N/A

   The Fraud, Analysis & Detection Solution Revise (FADSR) had an internal assessment, FTB security assessment, and Information Sharing and Analysis Center (ISAC) assessment completed within the past year. No findings – in compliance.

3. **Additional Assessment Criteria**

   If there is an existing Privacy Threshold Assessment/Privacy Information Assessment, include it as an attachment to your email submission.

   How many locations and total users is the project anticipated to affect?

   Number of locations: 1 location – FTB Central Office

   Estimated Number of Transactions/Business Events (per cycle): 21 million tax returns per year

   Approximate number of internal end-users: 20

   Approximate number of external end-users: 0

1.10 Funding

Planning

1. Does the Agency/state entity anticipate requesting additional resources through a budget action to *complete planning* through the project approval lifecycle framework? No

   If Yes, when will a budget action be submitted to your Agency/DOF for planning dollars?

Click or tap to enter a date.

2. Please provide the Funding Source(s) and dates funds for planning will be made available:

N/A

Project Implementation Funding

1. Has the funding source(s) been identified for *project implementation*? Yes

   If known, please provide the Funding Source(s) and dates funds for implementation will be made available:

   General Fund and Special Funds (to be confirmed), 07/2026

   Will a budget action be submitted to your Agency/DOF? Yes

   > If "Yes" is selected, specify when this BCP will be submitted: 08/16/2025 GovOps 08/30/2025 to DOF

2. Please provide a rough order of magnitude (ROM) estimate as to the total cost of the project: $10 to $15 million

End of agency/state entity document.

Please ensure ADA compliance before submitting this document to CDT.

When ready, submit Stage 1 and all attachments in an email to ProjectOversight@state.ca.gov.

Department of Technology Use Only

Original "New Submission" Date: 11/25/2024.

Form Received Date: 11/25/2024.

Form Accepted Date: 11/25/2024.

Form Status: Completed.

Form Status Date: 11/25/2024.

Form Disposition: Approved.

> If Other, specify: Click or tap here to enter text.

Form Disposition Date: 11/25/2024.

Department of Technology Project Number (0000-000): 7730-223.