STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 10/20)

Fiscal Year	Business Unit	Department	Priority No.
2022-23	7730	Franchise Tax Board	003

Budget Request Name	Program	Subprogram

Budget Request Description
Identity Proofing and Online Fraud Detection

Budget Request Summary
The Franchise Tax Board (FTB) requests $3.4 million, $3.3 million in General Fund and $86,000 in Special Fund, 17 permanent positions and 1 limited-term position in FY 2022-23; $2.9 million, $2.8 million in General Fund and $73,000 in Special Fund, 17 permanent positions in FY 2023-24 and ongoing to accommodate both new workloads and growth within the critical functions of policy, security, and disclosure that are a part of FTB's business processes utilizing a new identity verification tool for fraudulent calls and a threat behavior analytics tool.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed
☐ Yes ☒ No	

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO	Date

For IT requests, specify the project number, the most recent project approval document (FSR, SPR, S1BA, S2AA, S3SD, S4PRA), and the approval date.

Project No. **Project Approval Document:**

Approval Date:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By	Date	Reviewed By	Date
Department Director	**Date**	**Agency Secretary**	**Date**

Department of Finance Use Only

Additional Review: ☐ Capital Outlay ☐ ITCU ☐ FSCU ☐ OSAE ☐ Dept. of Technology

PPBA	Date submitted to the Legislature

A. Budget Request Summary

The Franchise Tax Board (FTB) requests $3.4 million, $3.3 million in General Fund and $86,000 in Special Fund, 17 permanent positions and 1 limited-term position in FY 2022-23; $2.9 million, $2.8 million in General Fund and $73,000 in Special Fund, 17 permanent positions in FY 2023-24 and ongoing to accommodate both new workloads and growth within the critical functions of policy, security, and disclosure that are a part of FTB's business processes utilizing a new identity verification tool for fraudulent calls and a threat behavior analytics tool.

B. Background/History

FTB serves the citizens of the State of California by helping taxpayers file tax returns timely, accurately, and pay the correct amount to fund services important to Californians. As such, we strive to make interactions with our customers as effortless as possible, while safeguarding our systems, and ultimately the public, from the effects of fraud.

Privacy, Security, and Disclosure Bureau (PSDB) develops and enforces security policies and procedures for the safety of FTB's employees and California citizens, and to ensure the security, confidentiality, integrity, and availability of FTB's information and information systems. These departmental policies and procedures guide staff in the analysis and assessment of security measures for the protection of FTB's facilities and information. They also detect, verify, and prevent unauthorized access to information technology systems, networks, and data.

FTB's Chief Security Officer (CSO) is responsible for the oversight and management of all aspects of information security. The CSO also promotes awareness of privacy and security issues among management and staff and ensures sound security principles are reflected throughout the organization's vision and goals. Subject matter experts within the PSDB provide technical security expertise to the department.

Capability	Mandate	Objective
Information Security	• SAM 5300 • IRS Pub 1075 • FTB Security Policy	• Protect FTB's information and information processing assets • Prevent and detect fraud, inappropriate use/access, and physical damage or loss • Apply information security intelligence to address new and evolving threats • Manage vulnerabilities within the information processing infrastructure • Manage threats and incidents impacting FTB's information resources • Safeguard FTB systems to protect and mitigate risks

In the News:

There have been a number of recent news stories about online fraud. It is hitting every industry from online shopping to financial institutions as well as various government services. Forbes published the following information on March 12, 2020 indicating fraudsters are:

- Stealing personal identifying information (PII) and login credentials;
- Creating digital identities that look legitimate and difficult to identify;
- Combining actual Social Security Numbers (often belonging to children, the elderly, or the homeless) with other information that appears valid, such as an address or other government-issued ID number;
- Merging existing information from several people into a new persona;
- Fabricating an entirely new "person" using a false Social Security Number.

In October 2016, in regards to an Internal Revenue Service (IRS) audit, the Inspector General stated, "The risk of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers… In this environment, it is incumbent upon the IRS to take every possible step to ensure the security of taxpayer account information[1]." FTB must meet the same taxpayer protection as the IRS as required in IRS Publication 1075 to ensure protection of PII.

Independent Security Assessment Finding:

In 2016, FTB commissioned an independent security assessment that identified a gap in the way FTB granted access for tax professionals accessing client information. This assessment identified the risk of incomplete verification of tax professional identity prior to disclosing taxpayer PII. FTB created an enhanced vetting process of Tax Professionals to remediate the finding.

As business process improvements and the customer experience is enhanced, it is critical that vetting processes and procedures across the enterprise are consistent and meet privacy and disclosure standards. Potential gaps not only puts taxpayer data at risk of an unauthorized disclosure, but also places FTB systems at risk.

FTB's Commitment to Detect and Mitigate Fraudulent Activities

FTB has a robust fraud detection program which monitors systems for unauthorized access attempts by bad actors and scrutinizes filed tax returns to address any identified questionable activity. Annually, the department stops over $132 million in questionable refunds. However, fraudulent activity has increased in complexity. To stay ahead of criminal activity, FTB requires additional staff and tools, such as identity verification and fraud deterrent systems, to improve and increase the prevention of dubious refunds.

FTB has redirected resources to address online fraud as feasible, as well as utilized two positions requested and received via a 2018-19 BCP, to begin addressing this emerging avenue for fraudulent activity. Several examples of outcomes include:

- In 2019, these staff opened 70 cases related to fraudulent activity, which affected almost 34,000 taxpayers. Fraudsters attempted to collect a total of almost $900,000 in fraudulent refunds. FTB was able to prevent $650,000 in payments for these fraudulent attempts.
- In 2020, these staff opened 65 cases related to fraudulent activity, which affected over 9,000 taxpayers. Fraudsters attempted to collect almost $120,000,000 in fraudulent refunds of which FTB prevented over $116,000,000 in improper payments for these fraudulent attempts.

FTB cannot continue to redirect resources to this workload without ongoing impacts to other critical security areas. Currently, FTB does not have the resources or robust tools to appropriately identify and address all the alerts that are triggered and the alerts are prioritized as High, Medium, and Low. On some days, staff can only timely review a portion of the alerts categorized as 'High'. The additional tools and positions will aid in refining current alert criteria to remove false positives and create automated processes to replace the current manual review processes. These resources and new software tools will ensure FTB, and the State, are well positioned to address significant risks associated with insufficient security protocols and staffing levels.

The positions and tools requested in this proposal will complement both of these work efforts that will now allow FTB to focus on security risks related to the one on one attempts to access account information on our systems wherein the bad actors are not trying to break through our security systems/firewalls, but are actually attempting to unlawfully use information they have illegally obtained to access our online self-service tools to either obtain additional

[1] https://www.treasury.gov/tigta/press/press_tigta-2016-25.htm

information or to engage in an activity that generates a refund. This third component has become critical to engage in as over the last decade numerous PII breaches have been reported and bad actors now have sufficient data to look like the 'real taxpayer' as they attempt to enter our online self-service tools. According to a government technology article released in January 2021, "five breaches each exposed one billion or more records and another 18 breaches exposed between 100 million and 1 billion records[2]." Workloads these resources will address can be generated by system detection tools or by FTB filing staff identifying and referring a suspicious tax return that appears to have a potential for wider scale fraud across a broad group of taxpayers which needs to be addressed. These requested additional staff will ensure that our systems allow authenticated taxpayers and professional's access but make every attempt to ensure bad actors are not allowed in.

Resource History

With the identified audit risk finding, FTB requested and received two positions in the FY 2018-19 Information Technology Security Enhancement BCP so that FTB could begin addressing the risk immediately, and also to understand the level of resources needed in the future to adequately address this risk. In the last several years, FTB has been able to develop metrics based on the current understanding of the risk, resource requirements, and workload. FTB is now prepared to request the additional resources to form a team to fully support this workload and protect FTB's online systems and taxpayers from fraudulent activity.

(Dollars in thousands)

Program Budget	2016-17	2017-18	2018-19	2019-20	2020-21 (P 06)	2021-22
Authorized Expenditures	$5,893	$9,006	$11,901	$12,687	$13,178	$13,178
Actual Expenditures	$5,893	$9,006	$11,901	$12,687	$6,389	0
Revenues						
Authorized Positions	48.0	72.0	97.0	97.0	96.0	96.0
Filled Positions	44.8	70.2	81.5	89.0	84.0	
Vacancies	3.2	1.8	15.5	8.4	12.0	0

C. State Level Consideration

FTB is responsible for administering the income tax program on behalf of the State of California. California's income tax program is a voluntary-based program relying on taxpayers to correctly self-report their income tax. Through these efforts, FTB collects approximately 74% of the General Fund revenue, equating to $92.3 billion; and processes 22.5 million returns and 14.6 million refunds annually[3]. It is vital FTB maintains the integrity and security of systems and data to ensure taxpayers self-comply and trust the safety and security of their personal and financial data reported on tax returns.

[2] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html

[3] Revenue figures based on the 2019-20 Cash Report reported in the Department of Finance's July 2020 Finance Bulletin. Due to the filing extension of April 15, 2020 to July 2020, the total revenue collected was lower than previous years.

Incidents of fraud are not only increasing, but are also becoming more clever and complex. This requires timely response and more in-depth analysis to understand the fraudulent activity, address the attack, and identify ways to avoid or mitigate future risk of a similar fraud scheme. As FTB expands online self-service applications that provide confidential and sensitive information, it is imperative FTB ensures the necessary monitoring and protection is in place to prevent fraudulent activity and financial loss to the state.

Goal 4: Operational Excellence states "Optimize our processes, products, services, and resources to better serve our internal and external customers." It is important to support and keep pace with FTB's growing technologies, programs, applications, and information systems. Adding new security measures will mitigate any associated security vulnerabilities that could burden California with additional outlays.

- Strategy 4.2: Validate and utilize data, as authorized, to make decisions and improve business operations.
- Strategy 4.3: Leverage and modernize IT systems and processes to support and improve business and administrative activities.
- Strategy 4.4: Mitigate emerging and evolving threats to manage risks and protect customer privacy and security.
- Strategy 4.5: Standardize and modernize our hardware and software to optimize operations.

This particular request mitigates emerging and evolving threats to manage risks and protect FTB systems and operations, as well as customer privacy and security.

D. Justification

FTB must remain vigilant in identifying fraudulent activity and abuse of online tools and applications to better protect taxpayer confidential and sensitive data. The information FTB collects, processes, and stores is extremely valuable to fraudsters engaging in identity theft and attempting to commit financial fraud. Identity theft fraud continues to grow and evolve. Rapidly changing technology continues to increase the volume and sophistication of threats, security breaches, attacks, and fraud schemes. FTB must mitigate identified risks due to new technology and instant access to all public-facing applications. Fraud results in substantial costs and impacts tax revenue as well as causes disruption of vital operations and a damaging loss of public trust. The additional funding will establish a dedicated team and deploy additional automated software tools allowing FTB to improve policies associated with this work; ensure verification of identity and access rights; increase compliance; provide centralized oversight; and overall enhance fraud detection.

Establish and Maintain Standardized Policies and Processes

FTB's efforts to provide access to taxpayer information through online services and applications increased the number of taxpayers, tax professionals, and information reporters requesting access. FTB has also assumed responsibility for many nontax related programs that require identity verification such as the Health Care Mandate and CalSavers collection efforts. FTB requires additional resources to support the workload growth and development to support these services. FTB intends to establish a dedicated team that will develop and maintain enterprise-wide identity verification policy, standards, processes, compliance monitoring, and tools for identifying and validating all taxpayers, tax professionals, and information reporters requesting access to FTB systems. Over that past few years there has been significant changes to privacy laws (NIST, IRS PUB 1075, CCPA, etc.) and we anticipate that privacy laws will continue to evolve. The dedicated team will be subject matter experts for policies and procedures that outside units will use as a resource to ensure compliance with changes in privacy laws through new legislation. The staffing increase for identity verification will provide

oversight and consistency throughout the enterprise and ensure FTB's compliance with laws and regulations.

As previously discussed in the Background section, in the last several years, FTB had redirected positions to address this critical work. However, this redirection is not sustainable as viable workloads are not being done elsewhere and the position authority must be returned to the originating business area. FTB is no longer able to absorb these hours that we have done in the last several years to address this critical risk to FTB operations and the State. Therefore, FTB is requesting resources in this BCP to fully fund this workload.

Identify, Verify, and Establish Relationships

Associate Operations Specialist – Two permanent positions
Staff Operations Specialist – One permanent position

The need for enhanced identity vetting processes has only grown and become more apparent over the last several years as fraud increases in volume and sophistication with more online self-service applications available. FTB has taken on several nontax initiatives (i.e. Heath Care Mandate, CalSavers, etc.) over the past two years that require identity verification. Establishing an enterprise group of staff to manage these workloads will ensure consistency in identity vetting and verification. It is critical to have a team monitoring and preventing fraudulent access and registration utilizing consistent processes for identity verification.

Mitigate Risk of Fraudulent and Inappropriate Activity – FTB online applications and systems

Information Technology Specialist – Twelve permanent positions
Information Technology Supervisor II – One permanent positions

In 2016, FTB implemented a new self-service tool called MyFTB. With the level of information included in MyFTB, FTB fairly quickly identified suspicious behavior in MyFTB and promptly took steps to mitigate the attack and introduced system changes to thwart future attacks. While necessary, these changes actually made MyFTB harder to access and over the last several years, FTB has been working to identify a solution that will allow the system to return to a more user friendly version but still ensure critical protections are in place. This BCP seeks resources and tools to adopt these ease of use opportunities with necessary security protocols in place. Historically, hackers attempt to enter FTB systems through firewalls and other lines of defenses; this continues today, however, fraudsters are also attempting access to the systems as 'valid' taxpayers. Both methods are driven by the selling of data on the black market. The reality of today's world is that fraudsters have access to sufficient data that FTB's systems may recognize them as a legitimate taxpayer. A new layer of complexity and resources are needed to research cyber details such as IP addresses, e-mail addresses, geo locations, etc., to detect bad actors attempting access to the systems. FTB identified a critical need to predict, detect, respond, and stop hackers and other criminals from bypassing and taking advantage of the systems and applications based on established metrics. Security intelligence tools, processes, and procedures identify patterns of normal user activity on FTB systems and applications and produce alerts and reports as the activity deviates from normal. The investigation and analysis of external activity alerts enables FTB to respond and stop fraudulent activities in a timely manner and assists in combating evolving fraud attempts.

Staff will also perform key functions related to data analysis and modeling and are required to work closely with the technical subject matter experts (SMEs/Investigators) to refine, update, develop, and continuously monitor external alerts for evolving fraud schemes. These staff members will possess the knowledge to understand the full size and scope of information that is accessed by external individuals, fraud schemes, patterns, and impacts to taxpayers and the state. The analyst and modeler will use graph analysis, which provides indicators of fraud. Using available data, new alerts will be established and existing alerts will be refined, updated and continuously monitored for improvement.

The requested supervisor position will supervise the increased staffing resources and oversee the new External Investigations & Identify Verification Unit. They will plan, organize, and direct

staff activities and establish goals and priorities. The position will review and monitor assignments to ensure staff work is completed accurately, efficiently, and timely; and in conformance with security policies and procedures. The incumbent will provide leadership, teambuilding, and mentoring of staff and ensure tracking and resolution of external system misuse cases, preventing contamination of information systems, and determining appropriate actions.

These positions, in general will not work on tax returns or refunds displaying suspicious activity. The existing Fraud team in the Filing Division will continue to perform this work. Any fraudulent returns identified by this team would be referred to and worked by the Fraud and Discovery Section (FADS) on a referral basis.

Security Operations Center

Information Technology Supervisor II – One permanent position

The incumbent will act as supervisor for the Security Operations Center day team staff in the Security Operations Section (SOS). The Information Technology Supervisor (IT Sup II) will supervise the increased staffing resources and oversee the day team Security Operations Center (SOC) operational functions related to network monitoring, vulnerability management, incident response, and system administration. The IT Sup II will develop work plans and schedules to meet operational needs of the day team SOC. With the incumbent's responsibility of the day to day operations of the day team SOC, it will allow the SOC manager to effectively lead the strategic direction of all the workloads unit, including the external monitoring and identity verification teams.

Mitigate Risk of Fraudulent and Inappropriate Activity – FTB Interactive Voice Response Phone System

Information Technology Specialist I – One limited-term position
Associate Operations Specialist – 100 hours overtime

FTB identified fraudulent activity and abuse occurring within the Interactive Voice Response (IVR) phone system. Verifying caller identity and authenticating through knowledge-based questions is difficult. Fraudsters have sufficient taxpayer data, gained from other data breaches and public data, enabling them to answer many of the security questions. For example, Fraudsters call the IVR and Taxpayer Services Section call center to request a Personal Identification Number (PIN) or a change of address to conduct fraudulent activities, or a request to release a refund. FTB launched a pilot program to better understand the scope of the problem which was successful in identifying fraudulent calls attempted on the IVR. FTB randomly chose 6,300 calls out of 330,000 for review during the pilot. Of those 6,300 calls, about 3%, or 200, were identified as suspicious warranting further review. Currently, FTB IVR handles over two million calls a year. Based on the results of the pilot, it is clear that fraudsters are attempting to exploit FTB call centers to further their criminal activity. Technology solutions funded with this proposal provide additional information to the call center agents that identify high risk calls. This would be an indicator for the call center agents to perform additional verification steps on these calls to reduce unauthorized disclosures and fraudulent activity. Additionally, the investigations team will receive referrals from the call center alerts to further analyze and correlate between other fraudulent activities in online systems.

E. Outcomes and Accountability

Enhancing the ability to detect and mitigate the risk of fraudulent activity and inappropriate use of FTB's expanding public applications, services, and IVR, and establishing oversight and centralizing taxpayer, tax professional, and information reporter identity verification for the enterprise will provide the following outcomes:

- Additional fraud prevention by responding to system alerts and case referrals;
- Reduced revenue loss for the state;

- Increased ability to proactively stop bad actors;
- Continuous and enhanced monitoring of online services;
- Timely deactivation of identified fraudulent accounts;
- Reduced volume of fraudulent refunds;
- Increased data modeling, forensic development, and user behavior analysis for developing, refining, and monitoring external alerts;
- Compliance with state and federal mandates and guidance on protecting and ensuring the privacy of confidential data;
- Reduced fraudulent calls to the IVR increasing our ability to service more taxpayers;
- Enterprise oversight for taxpayer, tax professional, and information reporter identity verification.

The management of resources received in this proposal will be the responsibility of the Chief of the Administrative Services Division or a delegate. The fiscal oversight of the resources will be the responsibility of the Chief Financial Officer.

F. Analysis of All Feasible Alternatives

Alternative 1: The Franchise Tax Board (FTB) requests $3.4 million, $3.3 million in General Fund and $86,000 in Special Fund, 17 permanent positions and 1 limited-term position in FY 2022-23; $2.9 million, $2.8 million in General Fund and $73,000 in Special Fund, 17 permanent positions in FY 2023-24 and ongoing to accommodate both new workloads and growth within the critical functions of policy, security, and disclosure that are a part of FTB's business processes utilizing a new identity verification tool for fraudulent calls and a threat behavior analytics tool.

Pros:

- Enables proactive measures to protect the state against tax fraud, identity theft, cybercrime, and insider threats;
- Increases investigation for early detection and timely response to incidents;
- Reduces and/or mitigates departmental risks of data breaches;
- Maintains compliance with state and federal mandates and guidance on protecting confidential data;
- Increases fraudulent account deactivation;
- Reduces fraudulent tax refunds;
- Improves security of critical assets and confidential taxpayer data;
- Improves identity verification tools for public-facing applications;
- Reduces the volume of fraudulent calls to the IVR and call center.

Cons:

- Increases FTB's expenditure and allocation from the General Fund.

Alternative 2: Approve $2.23 million ($2.18 million General Fund and $55,000 Special Fund) and 12 permanent positions in FY 2022-23; and $2.0 million ($1.95 million in General Fund and $50,000 in Special Fund) in FY 2023-24 and ongoing.

Eliminates enhanced detection and mitigation of risk for fraudulent activity and inappropriate use in FTB's IVR phone system. It also does not establish centralized identity verification and compliance monitoring for the enterprise.

Pros:

- Enables limited proactive measures to protect the state against tax fraud, identity theft, cybercrime, and insider threats;
- Increases investigation for early detection and timely response to incidents;
- Reduces departmental risks of data breaches;
- Maintains compliance with state and federal mandates and guidance on protecting confidential data;
- Minor increases to fraudulent account deactivation;
- Slight reduction to fraudulent tax refunds;
- Reduces the risk of data breaches;
- Minor improvements to critical assets and confidential taxpayer data security;
- Improves identity verification tools for public-facing applications;
- Provides prompt notifications in the event of a breach.

Cons:

- Increases FTB's expenditure and allocation from the General Fund;
- Security is not enhanced consistently;
- No centralized enterprise identity verification and compliance monitoring resulting in an ongoing gap that bad actors can infiltrate our various operations;
- Increase in unidentified fraudulent activity;
- Loss of state revenue.

Alternative 3: Do not approve.

Pros:

- No increase of FTB's expenditure and allocation from the General Fund

Cons:

- Outdated security;
- Noncompliance with state and federal mandates and guidance on protecting confidential data;
- No centralized enterprise identity verification and compliance monitoring;
- Loss of state revenue;
- No proactive measures to protect the state against tax fraud, identity theft, cybercrime, and insider threats;
- No decrease in fraudulent calls to the IVR;
- Increase in unidentified fraudulent activity;
- Increases departmental risks of data breaches;
- Overdue notifications in the event of a breach.

G. Implementation Plan

- June 2022 – All documents to establish permanent positions are prepared and approved by the FTB Budget Officer and forwarded to Department of Finance.
- June 2022 – Department of Finance notifies FTB of position approval.
- July 2022 – Permanent positions are established and FTB begins hiring.

H. Supplemental Information

None

I. Recommendation

Alternative 1: Approve $3.4 million, $3.3 million in General Fund and $86,000 in Special Fund, 17 permanent positions and 1 limited-term position in FY 2022-23; $2.9 million, $2.8 million in General Fund and $73,000 in Special Fund, 17 permanent positions in FY 2023-24 and ongoing to accommodate both new workloads and growth within the critical functions of policy, security, and disclosure that are a part of FTB's business processes utilizing a new identity verification tool for fraudulent calls and a threat behavior analytics tool. This proposal will reduce the risk and scope of a fraudulent activity and will allow FTB to meet current workload demands. FTB will be in compliance with departmental policy, as well as Federal statutes and regulations. It will accomplish the following:

- Establish policy, monitor compliance, and provide oversight of centralized and standardized taxpayer, tax professional, and information reporter identity verification for the enterprise.
- Enhance the detection and mitigate the risk of fraudulent activity and inappropriate use in FTB's expanding public applications and services with new tools, automation, data modeling, analysis, and investigations.
- Enhance the detection and mitigate the risk of fraudulent activity and inappropriate use in FTB's Interactive Voice Response (IVR) phone system by utilizing a multi-factor call center anti-fraud solution, which will create a new workload requiring calls identified as potential fraud to be further investigated.

BCP Fiscal Detail Sheet

BCP Title:

BR Name:

Budget Request Summary

Personal Services