**“Insert Company Here”**

**BSA/AML and OFAC Policy**Effective Date: XXXXXX, XX, XXXX

[1. OBJECTIVES 4](#_Toc29807155)

[1.1 General 4](#_Toc29807156)

[1.2 Purpose 4](#_Toc29807157)

[1.3 Scope 4](#_Toc29807158)

[1.4 Consequences of Non-Compliance 5](#_Toc29807159)

[2. DEFINITIONS 5](#_Toc29807160)

[3. POLICY REQUIREMENTS 6](#_Toc29807161)

[3.1 Overview 6](#_Toc29807162)

[3.2 Designation of BSA Officer and Governance Structure 7](#_Toc29807163)

[3.3 Internal Controls 8](#_Toc29807164)

[3.3.1 BSA/AML and OFAC Risk Assessment 8](#_Toc29807165)

[3.3.2 KYC Program 8](#_Toc29807166)

[3.3.3 Standards for Loan Disbursements, Payments, and Refunds 9](#_Toc29807167)

[3.3.4 OFAC Compliance 10](#_Toc29807168)

[3.3.5 Transaction Monitoring 10](#_Toc29807169)

[3.3.6 Referrals for Potentially Suspicious Activity 11](#_Toc29807170)

[3.3.7 Regulatory Reporting and Recordkeeping 12](#_Toc29807171)

[3.3.8 Information Sharing 13](#_Toc29807172)

[3.3.9 Mechanisms Designed to Monitor Ongoing Compliance 13](#_Toc29807173)

[3.4 Training and Development 14](#_Toc29807174)

[3.5 Independent Testing 15](#_Toc29807175)

[4. ROLES AND RESPONSIBILITIES 15](#_Toc29807176)

[5. EXCEPTIONS 17](#_Toc29807177)

[6. POLICY ADMINISTRATION 18](#_Toc29807178)

[6.1 Document Management 18](#_Toc29807179)

[6.2 Approval Management 18](#_Toc29807180)

[6.3 Related Documents 18](#_Toc29807181)

[6.3.1 Related Procedures 18](#_Toc29807182)

[6.3.2 Applicable Law and Regulations 18](#_Toc29807183)

# OBJECTIVES

## General

[Insert Company Here] (“Insert Company Here” or the “Company”), its senior management, and its Board of Directors (the “Board”) are committed to deterring customers, partners, and outside parties from using the Company as a conduit for illegal activity and to supporting [Insert Financial Institution Here]’s BSA/AML and OFAC compliance efforts.

This BSA/AML and OFAC Policy (“Policy”) and its program establish a framework for effective compliance with the BSA/AML and OFAC laws and regulations applicable directly to [Insert Company Here] or its business partners and to communicate its clear commitment to strong compliance culture.

Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”), the Bank Secrecy Act (“BSA”), and Office of Foreign Assets Control (“OFAC”) regulations require that U.S. persons comply with applicable anti-money laundering (“AML”) and sanctions regulations. [Insert Company Here] is not a “financial institution” (as defined in the BSA at 31 U.S. Code § 5312) and therefore is not required by law to implement a BSA/AML program. However, [Insert Company Here] has made a commitment to implement an effective BSA/AML program that incorporates the regulatory expectations of its bank partners, including regulations relating to Know Your Customer (“KYC”) program and Customer Identification Program (“CIP”), transaction monitoring, referrals of potentially suspicious activity, and a comprehensive sanctions screening process.

## Purpose

The purpose of the Policy is to ensure that a program is in place to detect, prevent, and report illicit criminal activities such as money laundering and terrorist financing, as well as to ensure adherence to sanctions laws. The program should seek to understand and manage such risks in a systematic fashion that is compliant with Bank policy, applicable laws, regulations and guidance, and serves the best interests of [Insert Company Here], the Bank and their collective customers.

## Scope

This Policy applies to all origination and servicing activities performed by [Insert Company Here] associated with the Bank’s products or services in accordance with its individual program agreement with [Insert Company Here].

This Policy applies to all Business Lines and relevant support personnel at [Insert Company Here] as well as third-party partners and vendors with whom [Insert Company Here] has entered into business arrangements for ongoing operational activities. [Insert Company Here] third-party relationships include payment processors, systems providers, bank partners, and consultants, among others.[[1]](#footnote-1)

## Consequences of Non-Compliance

[Insert Company Here] recognizes that non-compliance with BSA/AML and OFAC rules and regulations can expose the Company to substantial risk, potentially including civil or criminal penalties. All employees are responsible for understanding this Policy and undertaking any specific BSA/AML and OFAC compliance responsibilities assigned to them.

Non-compliance with, or violation of, the Policy’s requirements by employees may result in:

* Disciplinary action, including termination in appropriate cases; and/or
* Civil and/or criminal penalties.

Willful blindness to, or tipping off a customer about, a potential money laundering violation can expose the Company and individuals to potential liability.

# DEFINITIONS

**Money Laundering:** Money laundering is the movement of cash or cash equivalent proceeds derived from illegal or criminal activities (“illicit funds”) into, out of, or through the financial system in a manner that can give such funds an appearance of legality. Money laundering involves funds derived from criminal activities, including but not limited to drug trafficking, smuggling, human trafficking, fraud, and corruption. This typically occurs in three stages:

* Placement, during which illicit funds are introduced into the financial system without attracting the attention of financial institutions or law enforcement;
* Layering, during which illicit funds are moved through numerous layers of financial transactions in an attempt to disguise and/or conceal the true origin and ownership of those illicit funds; and
* Integration, during which the now seemingly clean funds are retrieved through apparently legitimate transactions.

**Office of Foreign Assets Control:** OFAC administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

**Terrorist Financing:** Terrorist financing involves the solicitation, collection, or provision of funds to support terrorist acts or organizations. Funds used to finance terrorist activities may be derived either from criminal activity or from legal sources (e.g., charities), and the nature of the funding sources may vary according to the type of terrorist organization.

This Policy does not distinguish between money laundering risk and terrorist financing risk, which are together referred to as “AML risk.”

**Tipping Off:** Tipping off means alerting a customer to suspicions of money laundering or disclosing to a customer confidential actions taken by the Company for BSA/AML and OFAC compliance purposes, such as filing a Suspicious Activity Report (“SAR”).

**Willful Blindness:** Willful blindness means turning a blind eye or consciously avoiding facts or suspicions of money laundering or terrorist financing.

# POLICY REQUIREMENTS

## Overview

Although [Insert Company Here] is not required by law to implement a BSA/AML program, [Insert Company Here] has made a commitment to implement an effective BSA/AML program that reflects its contractual obligations as a service provider and is consistent with the regulatory expectations of its bank partners. As a U.S. company, [Insert Company Here] understands that it must comply with OFAC requirements.

This Policy requires that [Insert Company Here] develop a BSA/AML and OFAC program that includes the following components:

* Designation of a BSA Officer and governance structure;
* Internal controls, including:
  + A BSA/AML and OFAC risk assessment;
  + KYC program;
  + Standards for loan disbursements, payments, and refunds;
  + OFAC compliance;
  + Transaction monitoring
  + Referrals for potentially suspicious activity;
  + Regulatory reporting and recordkeeping;
  + Information sharing;
  + Mechanisms designed to monitor ongoing compliance;
* Ongoing employee training and development; and
* Independent testing.

## 

## Designation of BSA Officer and Governance Structure

The Board designates an experienced and knowledgeable Chief Compliance Officer (“CCO”) as the BSA Officer, who has responsibility for day-to-day oversight of the Company’s BSA/AML and OFAC compliance. The Board ensures that the CCO has sufficient authority and resources to effectively execute all duties. The CCO reports directly to the Chief Executive Officer (“CEO”) and regularly apprises the Board and senior management of ongoing compliance with the BSA/AML and OFAC. The BSA Compliance Officer is designated as [Insert Company Here]’s responsible individual for day-to-day execution and oversight of the BSA/AML and OFAC programs including:

* Manage aspects of the [Insert Financial Institution Here] Bank Secrecy Act (BSA), Anti-Money Laundering (AML) and OFAC programs that are outsourced to the Partner.
* Participate in Partner governance routines including new product development
* Maintain proficient knowledge of the rules and regulations, including but not limited to, the Bank Secrecy Act (BSA), USA Patriot Act, and OFAC.
* Maintain awareness of industry tools, systems and processes that will keep program scalable and competitive.
* Coordinate the administration of independent auditor engagements and Partners testing requests.
* Regularly report health of program to [Insert Financial Institution Here] and Partner Committees
* Submit ([Insert Financial Institution Here]) BSA policy exception and exemption requests to [Insert Financial Institution Here]
* Oversee suspicious activity monitoring operations including maintenance of surveillance software systems
* Conduct suspicious activity investigations as needed
* Submit Suspicious Activity Report escalations to [Insert Financial Institution Here] as needed
* Manage fraud systems and operations as applicable
* Assist with annual review procedures that align with this role
* Oversee all efforts to conduct due diligence reviews of customers, strategic partners, employees, vendors, and contractors
* Manage watchlist screen and other KYC systems and processes including 314(a)
* Manage information sharing requests including Partners requests for info
* Monitor and track BSA-AML high-risk customers processes.
* Assist in annual review of procedures that align with this role
* Maintain BSA program documentation (Procedures, Risk Assessment requests, etc.)
* Assist in the administration of independent audits and Partners testing request.
* Identify, track and drive the correction of program deficiencies (Issues Management)
* Track BSA policy exception and exemption requests
* Plan and execute ongoing monitoring of FCC operations
* Administer BSA training program

## 

## Internal Controls

### BSA/AML and OFAC Risk Assessment

The CCO conducts an annual risk assessment to identify the Program’s inherent BSA/AML and OFAC risk and the effectiveness of its controls. In conjunction with performing the risk assessment, the CCO will adopt a risk assessment methodology to support [Insert Company Here]’s risk assessment and any related BSA/AML and OFAC compliance processes.

Consistent with the regulatory obligations of covered financial institutions, the risk assessment process assigns an inherent risk rating based on an assessment of customers, product and services, and geographic risks. The CCO then assesses the adequacy of the design and implementation of mitigating controls to determine the residual risk.[[2]](#footnote-2)

As part of this risk assessment, the CCO will:

* Identify the Company’s current overall BSA/AML and OFAC risk profile;
* Determine the adequacy and effectiveness of BSA/AML and OFAC controls;
* Evaluate the adequacy and application of BSA/AML and OFAC resources;
* Identify the existence of any unmitigated and/or unacceptable BSA/AML and OFAC risk; and
* If necessary, recommend and implement modifications to the BSA/AML and OFAC program (and the underlying strategy, policies, and procedures) to bring the Company’s BSA/AML and OFAC risk to an acceptable level.

The CCO reports the results of the BSA/AML and OFAC risk assessment to the Board for review and approval. The CCO makes the assessment available to other functions within the organization.

### KYC Program

[Insert Company Here]’s KYC program allows the Company to identify and verify the identity of its customers with reasonable assurance.

#### Customer Identification Program

[Insert Company Here]’s CIP is a fundamental control in preventing the Company from becoming involved in money laundering, terrorist financing, or sanctions violations. [Insert Company Here]’s policy is to collect the following identity information for all of its customers, all of whom are individuals (the Company does not accept legal entities or businesses as customers):

* Full legal name;
* Date of birth;
* Social Security Number (“SSN”); and
* Current physical U.S. street address.

In addition, [Insert Company Here] may collect information for other purposes that will deepen its understanding of customer identity. Examples could include mobile telephone numbers and device ID.

[Insert Company Here] will collect this information using its proprietary mobile application and will not open an account until it has verified this information (“customer verification”) through at least one of the following criteria:

* Images of photo identification documents provided by the customer;
* [Insert Company Here]’s existing CIP data (for repeat customers);
* Information provided by a credit reporting agency; and/or
* Data from external identity verification or fraud detection service providers approved by the CCO.

[Insert Company Here]’s policy is not to open an account for persons who fail customer verification.

The Company will never open an account for customers who:

* Are corporations or other entities;
* Give only a P.O. Box address;
* Give a foreign address;
* Do not provide each of the required pieces of information identified above;
* Have previously had an account closed by the Company for BSA/AML or risk/loss management reasons; or
* Are subject to U.S. sanctions (see section *3.3.4 OFAC Compliance* below).

[Insert Company Here] will ensure that it provides written notification to its customers of the USA PATRIOT Act’s customer identification requirements and will retain all CIP information for at least five years after the date of the customer’s most recent transaction or transaction attempt.

### Standards for Loan Disbursements, Payments, and Refunds

The Company understands that loans and monetary refunds to customers pose a potential risk for money laundering and/or terrorist financing. As a result, the Company will strictly adhere to certain standards surrounding loan disbursements, payments, and refunds, including the following:

* Loan proceeds may only be disbursed directly to the dental providers from whom the customers receive the treatments financed by their loans;
* Loan proceeds may not be disbursed to the customers or any other parties;
* The maximum amount of each loan is limited to the amount required for a given treatment;
* Customers may not make loan payments to [Insert Company Here] by cash or monetary instruments (i.e., cashier's checks, traveler's checks, and money orders) – they may through ACH transfers or by personal checks;
* Credit may not be refunded to an account other than the one from which the customer made the payment; and
* Credit may not be refunded to an individual other than the original customer.

### 

### OFAC Compliance

The CCO will establish controls to ensure that [Insert Company Here] complies with OFAC regulations to enforce economic and trade sanctions based on U.S. foreign policy and national security goals. The OFAC controls will apply to all parties with which the Company does business including, but not limited to, customers, suppliers, vendors, and [Insert Company Here] employees. The CCO will establish systems and procedures to ensure that the Company:

* Screens each customer against OFAC sanctions programs and the Specially Designated Nationals and Blocked Persons (“SDN”) List prior to approving a loan;
* Screens suppliers, vendors, and employees prior to conducting business with them;
* Updates internal OFAC lists in a timely fashion when the OFAC announces changes to sanctions programs and/or SDN List;
* Screens all existing customers, suppliers, vendors, and employees against the SDN List when the list is updated;
* Blocks or rejects transactions as appropriate under U.S. sanctions law; and
* Reports blocked and rejected items to OFAC and prepares annual reports to OFAC on the total of blocked funds.

All potential matches to the SDN list will be reviewed as appropriate and either cleared or escalated timely. If a potential match cannot be confirmed as a false positive it will be promptly escalated to [Insert Company Here] BSA Compliance Officer. Accounts or transactions that appear to be positive matches should be either blocked or rejected as appropriate.

If a match with the SDN list is confirmed, [Insert Company Here] BSA Compliance Officer will within one day of taking any action to reject or block an account or transaction, will provide notification to the [Insert Company Here] BSA Officer in order to enable the filing of a blocked assets or rejected transactions report to OFAC.

A comprehensive report of all blocked transactions through the annual period ending on June 30th of each calendar year shall be gathered and sent to the Bank in order to meet annual OFAC filing requirements.

### Transaction Monitoring

[Insert Company Here] utilizes both automated and manual systems to monitor customer activity and to detect unusual or potentially suspicious transactions. [Insert Company Here]’s policy is to take a conservative approach to monitoring by setting low dollar monitoring thresholds and by denying accounts that display unusual activity. At a minimum, the Company will monitor for:

* Loan payments by third parties;
* Sudden/unexpected payment on loans with no evidence of refinancing or other explanation;
* High volumes of loan applications at a single dental practice;
* High volumes of fraud claims associated with a given dental practice, both by dollar amount and number of transactions;
* Fraudulent loan applications;
* Excessive overpayments or refunds;
* Patterns that may indicate potential criminal activity; and
* Excessive accounts or transactions assigned to one SSN, address, or telephone number.

In addition, the Company requires all its employees to report unusual or potentially suspicious activity to the CCO, including but not limited to activity identified by fraud detection systems. The CCO will ensure that all employees receive training on how to report suspicious activity as part of the BSA/AML and OFAC training program (see section *3.4 Training and Development* below).

The CCO will set transaction monitoring thresholds and will have authority to make changes as needed in response to emerging patterns of activity. The CCO will document the reason for raising or eliminating a monitoring threshold and report that to the Risk Management Committee. The Board must also ratify lowering a monitoring threshold or imposing a new threshold. However, in the event that new patterns of suspicious activity emerge between meetings, the CCO is authorized to impose new thresholds pending the next Board meeting. The CCO will ensure that the rationale for all changes in thresholds is documented and retained.

### Referrals for Potentially Suspicious Activity

Under federal law, covered financial institutions must file a SAR when a transaction is suspicious. While [Insert Company Here] is not obligated to file SARs, its relationship with its bank partners requires that it refer potentially suspicious activities that it observes as part of the customer onboarding and monitoring processes.

[Insert Company Here] has implemented procedures for referring potentially suspicious activity to its bank partners and, consistent with BSA legal requirements, maintains records for customer account information (including the information obtained during the customer vetting process) for the time period required by federal obligations.

The CCO oversees investigations and determines whether the Company needs to take actions, including but not limited to, referral for potentially suspicious activity and account closure. Where a referral is not made, the Company will document the basis for that decision.

[Insert Company Here] will refer potentially suspicious activity to the relevant bank partner within 20 business days of reasonably becoming aware of the activity. The Company prohibits all employees from “tipping off” users that they are under investigation or that [Insert Company Here] has made referrals for their potentially suspicious activity.

In addition, the CCO may, at his or her discretion, alert law enforcement directly of activity that he or she believes will be of immediate use to a particular agency. Reportable unusual activity includes:

1. Criminal violations involving insider abuse in any amount (insiders include directors, officers, employees, agents or other institution affiliated parties);
2. Criminal violations aggregating $5,000 or more when a suspect can be identified;
3. Criminal violations aggregating $25,000 or more regardless of potential suspect;
4. Transactions conducted or attempted by, at or through and aggregating $5,000 or more if or the Bank suspects or has reasons to suspect the transaction:
   1. May involve potential money laundering or other illegal activity
   2. Is designed to evade the BSA or its implementing regulations
   3. Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and or the Bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

All information provided to the Bank to support these activities will be strictly confidential, including processes and controls within [Insert Company Here] to prevent unauthorized access or dissemination of such information.

Final SAR filing decisions and activities are entirely at the discretion of the Bank.

### Regulatory Reporting and Recordkeeping

#### Currency Transaction Reporting

The Currency Transaction Report (“CTR”) requirements do not currently apply to [Insert Company Here] because the Company does not accept currency as defined by the Internal Revenue Service (“IRS”).

If, due to a change in the IRS’s filing requirements or [Insert Company Here] business activities, [Insert Company Here] begins accepting currency as defined by the IRS, the CCO will amend this Policy and develop procedures for filing CTRs in accordance with the relevant regulations.

#### Purchase and Sale of Monetary Instruments Recordkeeping

The Company has no plans to purchase or sell monetary instruments.

If in the future the Company develops plans to do so, the CCO will ensure that the Company develops recordkeeping procedures in advance of commencing the activity.

#### 

#### Funds Transfer Recordkeeping

The Company allows customers and dental providers to make and receive funds transfers only through ACH payments, which are exempt from funds transfer recordkeeping requirements.

If in future the Company develops plans to allow other types of funds transfers, the CCO will ensure that the Company develops recordkeeping procedures in advance of the activity commencing.

#### Reports of International Transportation of Currency or Monetary Instruments (“CMIRs”)

The CMIRs requirements do not currently apply to [Insert Company Here] because the Company does not plan to undertake any activities that would involve transporting, mailing, or shipping monetary instruments out of or into the United States in any amount.

If in the future the Company develops plans to allow other types of funds transfers, the CCO will ensure that the Company develops reporting procedures in advance of the activity commencing.

### Information Sharing

The Company will cooperate fully with federal government authorities, law enforcement authorities, and financial institution partners on BSA/AML investigations to the extent allowable under applicable privacy and other laws.

The CCO will establish systems and procedures to ensure that the Company:

* Establishes a central process for receiving, documenting and responding to requests for information sharing and subpoenas; and
* Promptly evaluates all information sharing requests received, including those from its bank partners, and provides timely responses providing all information [Insert Company Here] is legally allowed to share.

### Mechanisms Designed to Monitor Ongoing Compliance

#### 

#### Staffing

The CCO will ensure that he or she has adequate staffing, both in numbers and qualifications, to implement the Company’s BSA/AML and OFAC program effectively. At least annually, the CCO will present his or her approach to staffing to the Risk Management Committee for approval and will ensure that all activities performed on behalf of the Company comply with Company policies and procedures and all applicable regulatory requirements regardless of the personnel performing the tasks.

#### 

#### New Products

New or modified products and business practices require, among other things, sign-off by the CCO through a separate process coordinated pursuant to the Company’s Compliance Policy and related procedure. The CCO evaluates the potential BSA/AML and OFAC risks of new or changed products and services from a compliance perspective to ensure that any BSA/AML and OFAC risks are appropriately identified and mitigated.

#### 

#### Quality Assurance/Testing

The CCO will put in place a regular quality assurance program to ensure that the Company maintains a high quality BSA/AML and OFAC program. At a minimum, this Quality Assurance Program will review the Company’s:

* KYC program;
* Quality of transaction monitoring;
* Timeliness and quality of referrals to bank partners;
* Information sharing;
* OFAC screening; and
* Recordkeeping.

The CCO will ensure that the approach to testing BSA/AML and OFAC compliance is consistent with the Company’s overarching compliance testing approach.

#### 

#### Reporting

To ensure effective management and Board oversight of the BSA/AML and OFAC Policy and program, the CCO reports quarterly to the Risk Management Committee and annually to the Board on:

* BSA/AML and OFAC compliance trends;
* BSA/AML and OFAC quality assurance/testing results;
* Material BSA/AML and OFAC compliance issues and/or escalated issues;
* Status of BSA/AML and OFAC corrective actions;
* Independent testing findings, bank partner concerns, and/or regulatory concerns; and
* Emerging BSA/AML and OFAC compliance issues which the Company will need to address.

The annual report to the Board on the state of BSA/AML compliance and any significant emerging issues will assist the Board in evaluating any Policy changes that may be appropriate.

[Insert Company Here] will provide the applicable reporting to the Bank in the timeframes agreed upon between the two parties. [Insert Company Here] will also provide any required reporting to demonstrate adherence to this Policy in a format and timeframe as deemed reasonable.

## Training and Development

The Company requires that all employees of both [Insert Company Here] and its third-party service providers, as well as the Board, receive BSA/AML and OFAC training appropriate to their roles and responsibilities. The first training will have to be within 30 days of start date after which employees need to complete training on an annual basis.

The goals of [Insert Company Here]’s BSA/AML and OFAC training program are to:

* Ensure [Insert Company Here]’s employees are familiar with relevant BSA/AML and OFAC requirements pertaining to their specific job functions and that they receive the most current information available;
* Ensure that the Board is knowledgeable regarding [Insert Company Here]’s obligations and responsibilities under BSA/AML law;
* Inculcate an understanding of the significance of [Insert Company Here]’s BSA/AML and OFAC compliance efforts and help develop a strong culture of compliance across the Company; and
* Develop a cadre of staff and managers throughout [Insert Company Here] to detect, escalate, and manage BSA/AML and OFAC compliance-related risks as and when they arise.

Consistent with [Insert Company Here]’s Compliance Policy, the CCO is responsible to ensure that the BSA/AML and OFAC training program is incorporated into the annual compliance training plan.

## Independent Testing

The Board oversees the completion, at least annually, of an independent test of [Insert Company Here]’s BSA/AML compliance by a qualified third-party firm, for assessing the implementation and effectiveness of the Company’s BSA/AML and OFAC Program and the adequacy of its controls over BSA/AML and OFAC compliance risk. The CCO is responsible for updating [Insert Company Here]’s risk assessment in light of any issues raised during the independent testing and taking necessary corrective action to remediate findings. The engagement will include, at a minimum:

* An evaluation of the overall effectiveness of the BSA/AML/Sanctions Compliance Program, including related Policies, SOPs, and processes
* Risk-based transaction testing to verify the adherence to BSA/AML/Sanctions recordkeeping and reporting requirements
* An evaluation of Management’s efforts to resolve violations and deficiencies noted in previous audits and/or regulatory examinations
* A review of BSA/AML staff training for adequacy, accuracy, and completeness
* A review of the effectiveness of the suspicious activity monitoring systems used for BSA/AML compliance.
* An assessment of the overall process for identifying and reporting suspicious activity to [Insert Financial Institution Here], including a review of filed or prepared SARs for accuracy, timeliness, completeness, and adherence to the Policy.
* An assessment of the integrity and accuracy of Management Information Systems (MIS) used in the BSA/AML/Sanctions Compliance Program.

Draft and final reports will be made available to the Bank and issues noted within the report will include [Insert Company Here] management response and will be tracked and remediated in a timely manner.

# ROLES AND RESPONSIBILITIES

|  |  |
| --- | --- |
| **Responsible Party** | **Roles** |
| Board of Directors | * Designate a BSA Officer; * Review this Policy and adopt revisions as necessary, no less than annually; * Approve the BSA/AML and OFAC risk assessment; * Oversee the Company's BSA/AML and OFAC program, assessing its effectiveness via an independent test by a qualified third-party firm at least annually; * Review compliance reports related to this Policy at least annually, including the state of compliance, testing and monitoring reports, and reports on complaint trends; * Review escalated issues related to this Policy; and * Identify and assess emerging compliance issues related to this Policy. |
| Risk Management Committee | * Ensure that the Company has sufficient compliance resources, including personnel and systems, to meet the Company’s objectives and to implement this Policy and its related program and make recommendations regarding enhancements to the CEO as necessary; * Review compliance reports related to this Policy at least quarterly, including the state of compliance, testing and monitoring reports, and reports on compliance trends; and * Review, approve, and oversee Company-wide initiatives related to this Policy and refer to the CEO for resolution any matter upon which there is material disagreement. |
| Policy Owner: Chief Compliance Officer | * Implement and maintain this Policy and related policies and procedures; * Approve exceptions to this Policy and maintain a written record of exceptions, including reasons for granting them; * Review and refresh the BSA/AML and OFAC program and the BSA/AML and OFAC risk assessment at least annually, and more frequently as circumstances require; * Oversee the implementation of the BSA/AML and OFAC program, including providing guidance and direction to senior management about the steps they need to take to institute the BSA/AML and OFAC program in their areas of responsibility; * Ensure that the Company fully meets its BSA/AML and OFAC compliance requirements in a timely fashion, including designing appropriate controls and conducting testing of their effectiveness; * Review any changes to BSA/AML-related laws, regulations, guidance, or supervisory expectations and ensure that the Company remains fully in compliance with its legal obligations and supervisory expectations; * Promptly alert the Board and Risk Management Committee to any material issues of BSA/AML and OFAC non-compliance, and institute and monitor corrective action; and * Provide periodic reporting to the Board and Risk Management Committee on the state of BSA/AML and OFAC compliance and any significant emerging issues. |
| Business Lines | * Communicate this Policy and its requirements to staff and third-party service providers within their area of responsibility; * Implement this Policy and other applicable policies and procedures within their area of responsibility; * Implement policies, procedures, and other controls to comply with new and revised laws and regulations related to this Policy; * Maintain systems, procedures, reports, and other controls used to support efforts to comply with this Policy; * Ensure that staff receive appropriate compliance training on this Policy; * Conduct monitoring activities to identify compliance weaknesses related to this Policy, and promptly alert and work with the CCO to take corrective action; and * Notify the CCO of proposals for new or modified products, services, initiatives or distribution channels. |
| Legal Counsel | * Interpret laws and regulations; * Provide advice and counsel regarding the requirements of applicable laws, regulations, and Company policies to all stakeholders; and * Review and approve all customer-facing documents, new or significantly revised products, services, and business practices. |
| Human Resources | * Assist the CCO with the development and administration of BSA/AML and OFAC training and maintain records of training attendance. |
| All Employees, Contractors, and Service Providers | * Know their responsibilities under this Policy; * Identify compliance weaknesses within their areas of responsibility related to this Policy, and promptly alert relevant senior management and the CCO; and * Grant the CCO, or designee, unrestricted access to business records, systems, or locations necessary to fulfil the duties described in this Policy. |

# EXCEPTIONS

From time to time, [Insert Company Here] may reasonably determine that a Policy exception is warranted. This Policy requires the CCO to sign off on any such exceptions and to provide reporting to the Risk Management Committee. For exceptions involving critical relationships, the CCO should advise the Board on potential risks associated with the exception as well as any proposed actions for mitigating risks. Certain exceptions should be escalated to [Insert financial Institution Here] for approval.

Notwithstanding the foregoing, under no circumstances does [Insert Company Here] allow Policy exceptions that would result in a violation of law.

# POLICY ADMINISTRATION

## Document Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modified Date** | **Modified By** | **Approved By** | **Revision** | **Version** |
|  | Chief Compliance Officer | Risk Management Committee |  | 1.1 |

## Approval Management

|  |  |  |
| --- | --- | --- |
| **Approved Date** | **Approved By** | **Version** |
| November 13, 2019 | Board | 1.0 |

## Related Documents

### Related Procedures

* BSA/AML and OFAC Procedures

### Applicable Law and Regulations

* The following are non-exclusive but key laws and regulations that apply to this Policy:
* Bank Secrecy Act, including the following:
  + 31 U.S.C. 5311-5332
  + 31 U.S.C. 1951-1959e
* Bank Secrecy Act Regulation, including the following:
  + 31 CFR Chapter X
* Office of Foreign Assets Control, including the following:
  + 31 CFR Part 500, *et seq.*
  + List of Specially Designated Nationals and Blocked Entities
* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”)
  + Public Law 107-56

1. Refer to the Third-Party Risk Management Policy for risk management of third-party relationships, including due diligence requirements for dental providers and partners. [↑](#footnote-ref-1)
2. Refer to the BSA/AML and OFAC Risk Assessment Methodology for additional details on this process. [↑](#footnote-ref-2)