# BSA/AML/OFAC Policy

|  |  |
| --- | --- |
| **Title:** | BSA/AML/OFAC Policy |
| **Scope:** | This Policy applies to all employees of COMPANY NAME |
| **Policy Owner:** | PLACEHOLDER |
| **Approved By:** | Board of Directors |
| **Effective Date:** | PLACEHOLDER |
| **Last Revision Date:** | PLACEHOLDER |

Table of Contents

[I. Overview and Purpose 3](#_heading=h.gjdgxs)

[II. Policy Statement 3](#_heading=h.30j0zll)

[III. Key Definitions 3](#_heading=h.1fob9te)

[IV. Roles and Responsibilities 5](#_heading=h.3znysh7)

[V. Policy Requirements 6](#_heading=h.2et92p0)

[A. Risk Assessment Framework 6](#_heading=h.tyjcwt)

[B. Designated BSA Compliance Officer 6](#_heading=h.3dy6vkm)

[C. Monitoring and Testing 6](#_heading=h.1t3h5sf)

[D. System of Internal Controls 7](#_heading=h.2s8eyo1)

[1. Customer Identification Program (“CIP”) 7](#_heading=h.17dp8vu)

[2. Customer Due Diligence 10](#_heading=h.3rdcrjn)

[3. Beneficial Ownership 10](#_heading=h.26in1rg)

[4. Adverse Media 11](#_heading=h.lnxbz9)

[5. Prohibited Customers 12](#_heading=h.35nkun2)

[6. Suspicious Activity Reporting 12](#_heading=h.1ksv4uv)

[7. Methods of Transaction Monitoring 13](#_heading=h.44sinio)

[8. Sanctions and Watchlist Screening 13](#_heading=h.z337ya)

[9. Information Sharing/Information Requests 14](#_heading=h.3j2qqm3)

[10. Record-Keeping 14](#_heading=h.3as4poj)

[E. Testing (Audit) 15](#_heading=h.1y810tw)

[F. Training 15](#_heading=h.4i7ojhp)

[VI. Use of Third Parties 16](#_heading=h.2xcytpi)

[VII. Penalties for Non-Compliance 16](#_heading=h.1ci93xb)

[VIII. Reporting 16](#_heading=h.3whwml4)

[IX. Record Retention and Recordkeeping 16](#_heading=h.2bn6wsx)

[X. Policy History 17](#_heading=h.qsh70q)

# Overview and Purpose

This Bank Secrecy Act (“**BSA”**) / Anti-Money Laundering (“**AML”**) / Office of Foreign Assets Control (“**OFAC**”) Policy (the “**BSA/AML/OFAC Policy**” or “**Policy**”) governs the COMPANY NAME (“**Company**”) program to combat money laundering, terrorist financing, fraud, and other improper conduct (collectively, “**financial crimes**”), and to comply with all sanctions program requirements. This Policy addresses the requirements of the laws and regulations to develop and implement an appropriate and effective set of AML and Counter-Terrorist Financing (“**CTF**”) internal controls and procedures to comply with applicable laws, regulations, and guidelines, including the statutory provisions of the BSA, Title III of the USA PATRIOT Act (“**Patriot Act**”), rules and regulations issued by OFAC, regulatory requirements of the Federal Deposit Insurance Corporation (“**FDIC**”), and any other relevant AML and CTF related regulations established by regulatory agencies where Company conducts business.

# Policy Statement

Company is committed to the fundamental goals of protecting its customers’ funds, the integrity of its sponsor Bank, its employees and its reputation. The purpose of this Policy is to communicate Company’s financial crimes compliance program, which is designed to detect, prevent, and remediate money laundering, financial crimes, terrorist financing, and other forms of illegal behavior.

The objective of this Policy is to ensure that Company’s BSA/AML compliance program reflects sound practices and that Company maintains compliance with all BSA/AML legal requirements to appropriately mitigate the risks of financial crimes. Any question regarding a potential conflict between this Policy and other Bank policies and/or contractual agreements should be immediately escalated to the Chief Compliance Officer (“**CCO**”).

# Key Definitions

**NOTE: The contents of this section are highly subjective and can be edited based upon client preference.**

**Account**

Pursuant to the Customer Identification Program (“**CIP**”), an “account” is a formal relationship to provide or engage in services, dealings, or other financial transactions, and includes a deposit account, a transaction or asset account, a credit account, or other extension of credit.

**Bank**

A regulated financial institution with whom Company has an agreement to provide or receive services in connection with Company’s service and product offerings.

**Beneficial Owner**

Any entity, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns twenty-five (25) percent or more of the equity interests of a legal entity customer; and a single individual with significant responsibility to control, manage, or direct a legal entity customer, including: (i) an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or (ii) any other individual who regularly performs similar functions. If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, twenty-five (25) percent or more of the equity interests of a legal entity customer, the beneficial owner for purposes of this Policy shall mean the trustee.

**Customer**

Any natural or legal “person”, including, an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal persons who opens or maintains an account. A customer also includes an individual who opens a new account for another individual who lacks legal capacity (such as a minor), and an individual who opens a new account for an entity that is not a legal person (such as a civic club). A customer does not include a person who does not receive Company services, such as a person or entity whose application is denied.

**Money Laundering**

The process by which the true origin and ownership of proceeds of illegal activities are concealed to make them appear legitimate. These transactions will typically conceal the true source of funds, disguise the ultimate disposition of the funds, eliminate any audit trail, appear as though the funds came from legitimate sources, and evade income taxes.

**OFAC**

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals applied to targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many economic and trade sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

**Specially Designated Nationals and Blocked Persons**

As part of its enforcement efforts, OFAC publishes a list of individuals and legal entities owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country‐specific. Collectively, such individuals and companies are called "Specially Designated Nationals" (“**SDN**”). Their assets are blocked and U.S. persons are generally prohibited from engaging in financial transactions with counterparties.

**Terrorist Financing**

Terrorist financing is the process by which terrorists fund their operations in order to perform terrorist acts and to achieve their goals. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

**Willful Blindness**

The action of a party to engage in “deliberate avoidance of knowledge of a fact or facts.” This includes situations wherein a party knows or has reason to suspect the source of funds in a transaction to be derived from illegal activities – or that the transaction is related to money laundering or other such illegal activity – yet continues to conduct the transaction. The BSA has established that willfully blind behavior may be punishable by both civil and criminal penalties. Similarly, failing to report potential money laundering or other such suspicious activity carries both civil and criminal liability.

# Roles and Responsibilities

**Policy Approver**

Company is required to have a written BSA/AML and OFAC compliance program that is approved by Company’s Board of Directors (“**Board**”); approval is to take place at least annually, with Board approval noted in the Board minutes. The Board is responsible for approving the content of this Policy and any substantive material revisions, while approval of non-substantive revisions is the responsibility of the CCO..

**Policy Sponsor**

The CCO is responsible for reviewing the underlying rationale for this Policy, including substantive revisions and/or retirement of the Policy.

**Policy Owner**

The Board has delegated to the CCO, responsibility for monitoring and reporting on compliance with this Policy. The CCO may delegate to others the authority to adopt, develop, and implement procedures and reporting to support this Policy.

**All** **Employees**

All Company employees are responsible for: (i) understanding and complying with applicable laws and regulations and this Policy, (ii) completing required compliance training and (iii) promptly reporting actual or suspected violations of laws or other requirements. Third‐party service providers, vendors, and subcontractors are likewise responsible for compliance with requirements set forth in this Policy.

# Policy Requirements

The BSA/AML and OFAC compliance program must be fully implemented and reasonably designed to meet the BSA and OFAC requirements; practices must coincide with Company’s written policies, procedures, and processes. The BSA/AML compliance program, commensurate with Company's risk profile, contains the following elements designed and implemented in accordance with the required BSA/AML compliance pillars.

## Risk Assessment Framework

**NOTE: Multiple ways to structure the framework.**

Compliance risk is identified as one of the principal risks incorporated into Company’s operations, with anti-money laundering and terrorist financing compliance included in the broader Compliance risk category. The compliance risk assessment at Company is designed to identify inherent customer, geographic, product/service and channel money laundering and terrorist financing risk, and assess the effectiveness of mitigating controls to operate at a level of residual risk acceptable to Company. Through the ongoing process of AML/BSA and OFAC risk assessments, Company is able to appropriately allocate resources, enhance training initiatives/requirements, and improve process controls.

At least annually, the CCO will perform an enterprise‐wide assessment of the money laundering and terrorist financing risk at Company. An OFAC risk assessment is performed concurrently as part of the BSA/AML risk assessment process at Company.

## Designated BSA Compliance Officer

Company’s Board is required to designate one or more persons to coordinate and monitor day-to-day compliance. In this capacity, the CCO is designated to serve as the BSA Compliance Officer at Company

## Monitoring and Testing

Company conducts risk‐based compliance testing and monitoring of the performance of its BSA/AML compliance program commensurate with its activities and risk profile and provides for regular testing of the BSA/AML policies, procedures, and processes at Company. The monitoring and testing performed, based on the level of risk identified, factors: periodic compliance risk assessments, results of ongoing monitoring and testing, third‐party reviews conducted, and any changes to BSA/AML related processes.

### Compliance Monitoring

Compliance monitoring of Company activities is performed to ensure ongoing compliance with Company policies and processes. Ongoing monitoring enables the CCO to identify potential deficiencies in Company’s compliance with the BSA/AML and OFAC program in a timely manner.

### Compliance Testing

Compliance testing of Company activities is performed to periodically test and evaluate Company’s adherence to established BSA/AML and OFAC policies, procedures, and processes. The scope and level of transaction testing utilized in the compliance testing cycle is determined based on the results of the BSA/AML and OFAC risk assessment, compliance monitoring, and through discussions with executive management. Company will ensure that, at a minimum, processes related to the Company’s CIP, OFAC screening, and SAR investigation and filing will be tested at least annually.

## System of Internal Controls

The Board of Directors and Executive Management at Company are required to create a culture of compliance to ensure staff adherence to BSA/AML and OFAC policies, procedures, and processes. Internal controls are the policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of Company’s internal controls should be commensurate with the size, structure, risks, and complexity of Company. Due to the limited number of products offered by Company, the risks and compliance requirements at Company are not unique to any particular line of business or department, and are therefore universally applied to ensure a comprehensive BSA/AML and OFAC compliance program.

### Customer Identification Program (“CIP”)

Under Section 326 of the USA PATRIOT Act, Company has implemented a written Customer Identification Program to confirm the identity of any customer opening an account with Company. Section 326 requires that, at a minimum, KYC/CIP supplementary procedures are implemented by Company in order to:

* Verify the identity of any person seeking to open an account to the extent reasonable and practicable;
* Maintain records of the information used to verify the person’s identity, including name, address, and other identifying information; and
* Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to Company by any government agency.

This CIP policy governs Company’s requirements for identifying customers when opening accounts, utilizing appropriate methods to verify identification, performing customer due diligence, and retaining all required records. If the applicant does not provide the information required or does not submit the required identification to establish its true identity, Company will not render the service or establish the account.

#### Customer Verification Requirements for Individuals

**NOTE: Many variables can be considered.**

In compliance with CIP requirements, the information obtained[[1]](#footnote-1) and leveraged for customer identification and verification must contain the following – which Company shall maintain on file:

* Full Name, including prior names or aliases if known;
* Date of birth;
* Address**[[2]](#footnote-2)** (or permanent residence (foreign address) if the individual is foreign);
* Identification number**[[3]](#footnote-3)**; and
* Individual’s country of origin/citizenship (if the individual is foreign).

#### Customer Verification Requirements for Existing Customers

For existing customers opening a new account, Company will ensure the current information on file is verified by the customer or applicant during the application process and updated if required.

#### Taxpayer Identification Requirement

An account relationship with a U.S. person, as defined in Section 326 of the USA PATRIOT Act, will not be established until the required SSN/TIN or EIN information is obtained and registered. If an applicant does not have a SSN/TIN, they must provide evidence of application for a Tax ID. Accounts are not opened by Company for individuals lacking an SSN/TIN.

#### Acceptable Methods of Customer Identification

To meet regulatory requirements and expectations for confirming the identification of parties with whom Company will provide products and services to, the following methods exist:

##### Documentary Methods of Verification

Primary identification must evidence a customer’s nationality or residence and bear a photograph or similar safeguard. Examples include a driver’s license or passport. However, other forms of identification may be used if they enable Company to form a reasonable belief that it knows the true identity of the customer. For a “person” other than an individual (such as a corporation, partnership, or trust), Company is to obtain documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

##### Non-Documentary Methods of Verification

Non-documentary methods may include contacting a customer; independently verifying the customer’s identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement. If electronic credentials are utilized, they must be in accordance with the FFIEC’s Guidance “Authentication in an Electronic Banking Environment[[4]](#footnote-4).”

##### Acceptable Verification through the Combination of both Documentary and Non-documentary Methods

Company’s staff may be required to leverage a combination of documentary and non-documentary methods of verification, however this method applies only when Company cannot verify the customer’s true identity using other methods, including customers who are legitimately unable to present customary forms of identification. Under such circumstances, staff are required to properly document in the customer profile why standard CIP requirements were not followed, as well as to document what steps were taken instead to otherwise verify identity. This must also include the accompanying exception approval from the CCO or their designee.

#### CIP Customer Notice

Prior to opening an account, the applicant will be provided adequate notice that information verifying the customer’s identity will be requested. These notices will either be printed directly on account applications, posted in a conspicuous location on Company or an affiliate’s website, or provided orally for phone applications. For joint accounts, providing notice to one owner for delivery to the other owners is permitted. The regulation provides the following sample language[[5]](#footnote-5) that will be used:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver’s license or other identifying documents.

#### CIP Third-Party Reliance

The CIP rule does not alter Company’s authority to use a third party, such as an agent or service provider, to perform services on its behalf. Company may arrange for a third party, acting as its agent in connection with an account application, to verify the identity of an applicant. Company may also arrange for a third party to maintain its records. In the event Company elects to utilize third parties to perform any or all aspects of its customer verification processes, any applicable third parties are legally obligated to adhere to CIP requirements.

### Customer Due Diligence

A cornerstone of this Policy is Company’s Customer Due Diligence (“**CDD**”) program. The CDD program applies to all customers. Company recognizes that it is of paramount importance to know the customer’s business or professional activities, sources of the customer’s income, wealth or assets, and the particular source of the funds that are the subject of transactions at Company. It is also essential to understand how Company’s products and services fit into the customer’s stated objectives in order for Company to develop a customer risk profile.

A customer risk profile refers to the information gathered about a customer at account opening used to develop a baseline against which the customer activity is assessed for suspicious activity reporting. This may include self-evident information such as the type of customer or type of account, service or product. The profile may, but is not required to, include a system of risk ratings or categories of customers.

The risk profile of the customer considers the following attributes:

* Purpose of the account (all are consumer transaction accounts)
* Actual or anticipated activity in the account
* Nature of the customer’s business/occupation, relative to those identified as “high risk”
* Customer’s location
* Types of products and services used by the customer

In addition, CDD includes conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

### Beneficial Ownership

The Financial Crimes Enforcement Network (“**FinCEN**”) has established beneficial ownership identification rules via appendix to 31 C.F.R. § 1010.230 and 1020.210(b)(5) effective May 11, 2018. The law requires that banks, credit unions, securities broker/dealers, mutual funds, futures commission merchants; and introducing brokers in commodities enhance their due diligence practices when opening new accounts for legal entity customers (Corporations, Partnerships, Non-Profits, Sole Proprietorships, Trusts, etc.) by obtaining and maintaining information identifying the beneficial owners of legal entity customers.

### Adverse Media

**NOTE: Many variables to consider.**

In accordance with this Policy, Company’s CCO maintains the responsibility to recommend certain existing customers for account closure where permitted by law, including existing customers who have been convicted of the following crimes, when Company becomes aware of such information:

* Money Laundering or Bank Secrecy Act Violations;
* Terrorism and/or Terrorist Financing;
* Drug Trafficking;
* Human Trafficking and/or Human Smuggling;
* Bank, Mail, Securities, Check, or Wire Fraud;
* Identify Theft;
* Forgery;
* Embezzlement;
* Tax Evasion;
* Bank Robbery;
* Grand Larceny;
* Political Corruption or Bribery under U.S. or foreign law; or
* Organized Crime.

### Prohibited Customers

**NOTE: Many variables to consider.**

Company prohibits relationships with individual customers that are outside of Company’s risk tolerance. Specific examples of such individuals include, but are not limited to, the following:

* SDNs or other parties listed on the OFAC Consolidated Sanctions List; and
* Individuals whose identities cannot be verified during the customer verification process.

### Suspicious Activity Reporting

**NOTE: Requirements can change depending on whether the institution itself is responsible for filing SARs or if a partner bank bears responsibility.**

Financial institutions must monitor for suspicious activity and file Suspicious Activity Reports ("**SARs**"). The purpose of the SAR is to report known or suspected violations of federal law, or known or suspicious transactions related to criminal activity, including money laundering and terrorist financing. Potentially suspicious activity will be referred to Company’s partner Bank for potential SAR filing, should Company become aware of any of the following criteria:

* The transaction appears to involve funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;
* The transaction is designed to evade any regulations promulgated under the BSA;
* The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Company’s partner Bank is responsible for filing SARs on transactions that meet certain thresholds. As a result, if Company becomes aware of suspicious activity that meets any of the criteria defined above, Company will refer the activity to its partner Bank if the transaction(s) involve:

* Insider abuse in any amount; or
* Aggregate to $5,000 or more when a suspect can be identified; or
* Aggregate to $25,000 or more regardless of a potential suspect.

SARs are highly confidential and Company has implemented safeguards to prevent alerting the named subject by disclosing the existence of a SAR to anyone other than the partner Bank and FinCEN.

### Methods of Transaction Monitoring

**NOTE: Discretion as to how monitoring is conducted.**

Financial institutions must implement system(s) and processes that identify suspicious activity. Based on implemented methods, Company is required to immediately escalate all identified potentially suspicious activity to its partner Bank for SAR filing. The level of suspicious activity monitoring is dictated by Company’s risk assessment, with emphasis on product risk, customer risk, and geographic risk.

#### Automated Methods

Company will identify appropriate “red flags” and develop transaction monitoring surveillance and detection scenarios that seek to identify unusual activity using a risk-based approach according to the risk profile, products, services, customer base, geographic factors, and purpose of the transaction. Automated transaction monitoring methodology shall be consistent with regulatory guidance for model risk management.

#### Manual Methods

Company shall, as needed, utilize manual transaction monitoring methods, such as review of transaction reports or based on the results of due diligence reviews, adverse information, and employee referrals.

### Sanctions and Watchlist Screening

**NOTE: Discretion as to how screening is conducted.**

Company is committed to full compliance with the sanctions programs administered by OFAC, and other economic sanctions programs which may apply. Company shall establish reasonable procedures to determine whether an applicant or an existing customer appears on any list of known or suspected terrorists or terrorist organizations provided by any government agency as required by the regulatory statute.

Company must ensure that it does not engage in unauthorized business, or maintain unauthorized relationships, with persons that appear on a sanctions list maintained by a government agency that administers an applicable sanctions program, or that are in a jurisdiction targeted by a comprehensive sanctions program. Accordingly, Company conducts regular screening of applicants, customers and beneficial owners against OFAC's SDN List, and other applicable sanctions lists (collectively, "**Sanctions Lists**"). Any updates to the Sanctions Lists are incorporated into the screening process in a timely manner.

In all cases, if Company identifies a true “hit” on any actions Sanctions Lists, the CCO (or designee) will thoroughly review the account to determine appropriate steps, including escalation to its partner Bank for FinCEN and OFAC reporting.

### Information Sharing/Information Requests

#### Law Enforcement Inquiries and Requests

Company is responsible for responding to Section 314(a) requests, law enforcement inquiries, grand jury subpoenas and National Security Letters (“**NSLs**”).

Section 314(a) of the USA PATRIOT Act requires that financial institutions comply with requests for information from FinCEN regarding certain individuals suspected of terrorism or money laundering (“subjects of interest”). Upon receiving a Section 314(a) information request, Company must search for any accounts maintained by the named subject during the preceding twelve (12) months or any transactions involving the named subject conducted within the previous six (6) months. Positive matches must be reported to FinCEN within fourteen (14) days. When Company identifies subjects of law enforcement requests, the transactional activity in the account is reviewed to identify common relationships and/or suspicious activity. Any unusual and or suspicious activity identified as a result of a 314(a) search requires a SAR filing referral to Company’s partner Bank(s). If a SAR is required based on a law enforcement inquiry, the SAR may not in any way refer to the request itself but rather to the facts and activities that support the suspicious activity. 314(a) Information Requests and the 314(a) subject list are highly confidential, and financial institutions are prohibited from disclosing the fact that FinCEN has requested or obtained information to the account holder.

Certain law enforcement requests are highly confidential documents. As such, these inquiries, other than 314(a) requests, will be processed and maintained only by Company’s CCO. The information will be maintained in an electronic file with limited access.

#### Point of Contact

Company will designate a point of contact for Section 314(a) information sharing. Company does not participate in 314(b) information sharing.

## Testing (Audit)

Company shall conduct independent testing of compliance with its BSA/AML obligations every twelve (12) to eighteen (18) months, commensurate with Company’s BSA/AML and OFAC risk profile, size, complexity, scope of activities, quality of control functions, geographic diversity, and use of technology. The independent testing shall be conducted using outside auditors, consultants, or other qualified independent parties (e.g., qualified employees who are not involved in the function being tested). No outside auditors or consultants performing independent testing shall be involved in other BSA/AML or OFAC functions such as training or developing policies and procedures that may present a conflict or lack of independence. Independent audit findings are reported directly to the Board and Company executive management.

The scope of the independent testing includes an evaluation of the quality of risk management within all of Company’s operations, including oversight of third‐party service providers. The engagement also includes:

* An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes;
* A review of Company’s risk assessments for reasonableness given Company’s risk profile – customers products, services, customers, channels, and geographies – which are noted to be limited due to the limited nature of products/services offered and of customers/entities/geographic locations currently served;
* Risk‐based transaction testing to verify Company’s adherence to BSA recordkeeping and reporting requirements;
* An evaluation of management’s efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if any;
* A review of staff training for adequacy, accuracy, and completeness;
* A review of the suspicious activity monitoring reports and KYC systems (manual, automated, or a combination) used for BSA/AML compliance, to the extent these processes are executed by Company;
* An assessment of the overall process for identifying and reporting suspicious activity, including when and where the process is to refer any observed suspicious activity to Company’s partner Bank;
* An assessment of the overall process for identifying and escalating OFAC matches to Companys partner Bank; and
* An assessment of the integrity and accuracy of management information used in the BSA/AML compliance program.

## Training

**NOTE: Discretion as to how training is conducted.**

Company’s CCOr will determine the compliance training needs for all employees commensurate with job levels and responsibilities. All employees will receive the appropriate training at least annually. BSA, AML, and OFAC training will be included in Company’s mandatory new-hire training, to be completed within thirty (30) days of the start date of employment.

The training schedule is reviewed and approved by the CCO each year. They, or their designee, will ensure all applicable personnel (including the Board, employees, and contractors) have received the required training on BSA, AML, and OFAC requirements and responsibilities and have been documented. All training and testing materials, dates of training sessions, and attendance records are maintained for each training session. Periodic reporting of training progress, updates to any training initiatives, and any training issues are made to Company’s Board.

Company may place reliance on additional third-parties approved by its partner Bank to perform certain BSA/AML functions relating to customers, including CIP, CDD, and OFAC screening.

# Penalties for Non-Compliance

Penalties for money laundering and terrorist financing can be severe, and are among the highest criminal and civil penalties of any banking laws or regulations. Failure to comply with BSA/AML regulations and requirements may subject Company to supervisory action by federal regulatory agencies, as well as civil and criminal prosecution. Violations include the unauthorized disclosure of a SAR filing. The penalties include large monetary fines, forfeiture of property, and even imprisonment.

As a condition of employment, Company employees are required to adhere to applicable laws and regulations including BSA/AML compliance mandates. Employees are required to promptly report any concerns or possible breaches of laws, rules, regulations and/or applicable sanctions-related policies and procedures, including this Policy.

# Reporting

On an annual basis or more frequently as circumstances dictate, the CCO will present a report to the Board. This report will include insight into ongoing compliance initiatives, any deficiencies/corrective action noted, SAR filings/referrals relating to financial crimes compliance, and other key risk indicators (“**KRIs**”) and key performance indicators (“**KPIs**”) to enable informed decisions for BSA, AML, and Sanctions related matters.

# Record Retention and Recordkeeping

## 

## CIP

The BSA as well as Section 326 of the USA PATRIOT Act require institutions to create or obtain and then preserve certain records relating to customer information and transactions for potential examination by regulators, law enforcement and other government agencies. To comply with these established recordkeeping requirements, Company’s CIP requires that identifying information (name, date of birth, address, and tax identification number) obtained at the time of account opening shall be retained in accordance with regulatory requirements.

Company has established procedures for maintaining records of the identifying information, which require that the following data be retained according to Company’s Record Retention Policy after the record is created:

* Customer identifying information, including name, address, DOB, and TIN/SSN;
* A description of the type of any document reviewed for verification (Driver’s license, Passport, etc.);
  + The identification number on the document;
  + Place of issuance;
  + Date issued, if any;
  + Expiration date, if any;
* A description of any non-documentary methods used and results; and
* A description of how any substantial discrepancies were resolved.

For any extension of credit in excess of $10,000 (not secured by real property), the following shall be obtained, recorded, and kept on file for a minimum of five (5) years after the account is closed:

* Name of borrower;
* Address of borrower;
* Amount of credit extended;
* Nature or purpose of loan; and
* Date of loan.

Company will retain all applicable records (both electronic and physical) for the time period necessary to comply with requirements outlined in Company’s record retention policy. In general, all records will be retained for at least five years.

## Funds Transfers

Funds transfer recordkeeping requirements stipulate that each bank involved in funds transfers must collect and retain certain information in connection with funds transfers greater than $3,000. The information required to be collected and retained depends on the bank’s role in the particular funds transfer (originator’s bank, intermediary bank, or beneficiary’s bank). The requirements may also vary depending on whether an originator or beneficiary is an established customer of a bank and whether a payment order is made in person or otherwise.

Company maintains its own internal ledger that documents information related to funds transfers in and out of Company accounts. Company retains the information on these transfers indefinitely.

## Suspicious Activity Reporting Referrals

All records pertaining to referrals made to the partner Bank for potential SAR filings will be maintained for at least five (5) years.

## Sanctions List Escalation Referrals

All records pertaining to referrals made to the partner Bank regarding “true hits” identified in sanctions list screening (including OFAC) will be maintained for at least five (5) years.

## 314(a) Requests

All records pertaining to law enforcement requests made under Section 314(a) of the USA PATRIOT Act will be maintained for at least five (5) years.

# Policy History

The history of this document is outlined in the table below.

|  |  |  |
| --- | --- | --- |
| Date of Action | Responsible Party | Description of Policy Action |
| PLACEHOLDER | PLACEHOLDER | Version 1.0 |

1. Company may obtain identifying information from a third-party source before extending credit. [↑](#footnote-ref-1)
2. For an individual: a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer’s physical location. For a “person” other than an individual (such as a corporation, partnership, or trust): a principal place of business, local office, or other physical location. [↑](#footnote-ref-2)
3. An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and an identification number for a non-U.S. person is one or more of the following: a TIN; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. TIN is defined by section 6109 of the Internal Revenue Code of 1986 (26 USC 6109) and the IRS regulations implementing that section (e.g., Social Security number (SSN), individual taxpayer identification number (ITIN), or employer identification number). [↑](#footnote-ref-3)
4. <https://www.ffiec.gov/pdf/authentication_guidance.pdf> [↑](#footnote-ref-4)
5. <https://www.ecfr.gov/cgi-bin/text-idx?node=se31..1020_1220> [↑](#footnote-ref-5)