[Insert Company Logo Here]

Bank Secrecy Act Policy  
[Insert Financial Institution Here]|[Date]

Contents

[Background and Policy Statement 3](#_Toc508424317)

[Board Oversight 4](#_Toc508424318)

[BSA/AML Compliance Program Components 4](#_Toc508424319)

[BSA/AML Risk Assessment 4](#_Toc508424320)

[Internal Control Requirements 5](#_Toc508424321)

[Independent Testing Requirements 6](#_Toc508424322)

[BSA Officer Responsibilities 7](#_Toc508424323)

[Training Requirements 7](#_Toc508424324)

[CIP | Documents Required for Individuals 9](#_Toc508424325)

[CIP | Documents Required for Businesses 10](#_Toc508424326)

[CIP | Non-Documentary Verification Methods 10](#_Toc508424327)

[CIP | Additional Identification Procedures for Specific Customers 11](#_Toc508424328)

[CIP | Circumstances under which the Bank should Not Open an Account 11](#_Toc508424329)

[CIP | Exceptions 12](#_Toc508424330)

[CIP | When the Bank Should File a SAR 12](#_Toc508424331)

[CIP | Comparison with Government Lists 12](#_Toc508424332)

[CIP | Providing Customer Notice 12](#_Toc508424333)

[CIP | Reliance on another Financial Institution 12](#_Toc508424334)

[CIP | Use of Third Parties 13](#_Toc508424335)

[CIP | Record Retention 13](#_Toc508424336)

[Customer Due Diligence 13](#_Toc508424337)

[CDD | Identifying Beneficial Owners 14](#_Toc508424338)

[CDD | Determining a Customer’s Risk Rating 16](#_Toc508424339)

[CDD | Enhanced Due Diligence for Higher-Risk Customers 17](#_Toc508424340)

[CDD for Lending Relationships 17](#_Toc508424341)

[CDD | High Risk Banking Functions 17](#_Toc508424342)

[Suspicious Activity Reporting 17](#_Toc508424343)

[SAR Filing Requirements 18](#_Toc508424344)

[Suspicious Activity Reporting Safe Harbor 19](#_Toc508424345)

[Systems to Identify, Research and Report Suspicious Activity 19](#_Toc508424346)

[Identification of Unusual Activity 19](#_Toc508424347)

[Managing Alerts 20](#_Toc508424348)

[SAR Decision-Making Process 20](#_Toc508424349)

[SAR Filing on Continuous Activity 20](#_Toc508424350)

[SAR Completion and Filing 21](#_Toc508424351)

[Notifying the Board of SAR Filings 21](#_Toc508424352)

[Closing an Account Due to Continuous Suspicious Activity 21](#_Toc508424353)

[Prohibition of SAR Disclosure 21](#_Toc508424354)

[Documentation of Circumstances in which SARs have been considered, but Not Filed 22](#_Toc508424355)

[Suspicious Activity Reporting Record Retention 22](#_Toc508424356)

[Currency Transaction Reporting 22](#_Toc508424357)

[Aggregation of Currency Transactions 22](#_Toc508424358)

[CTR Completion and Filing 23](#_Toc508424359)

[Currency Transaction Reporting Exemptions 23](#_Toc508424360)

[Safe Harbor for Failure to File CTRs 25](#_Toc508424361)

[CTR Exemption Record Retention 25](#_Toc508424362)

[Information Sharing under the USA PATRIOT Act 25](#_Toc508424363)

[Section 314(a) Information Sharing 25](#_Toc508424364)

[Section 314(b) Information Sharing 26](#_Toc508424365)

[Purchase and Sale of Monetary Instruments 26](#_Toc508424366)

[Recordkeeping Requirements for Monetary Instrument Sales 27](#_Toc508424367)

[Funds Transfers 27](#_Toc508424368)

[Funds Transfer Recordkeeping 29](#_Toc508424369)

[Foreign Correspondent Account Recordkeeping, Reporting & Due Diligence 29](#_Toc508424370)

[Private Banking 30](#_Toc508424371)

[Special Measures under the USA PATRIOT Act 30](#_Toc508424372)

[International Transportation of Currency or Monetary Instruments Reporting 30](#_Toc508424373)

[Report of Foreign Bank and Financial Assets 31](#_Toc508424374)

[OFAC 31](#_Toc508424375)

[OFAC | Blocked Transactions 31](#_Toc508424376)

[OFAC | Prohibited Transactions 32](#_Toc508424377)

[OFAC | Licenses 32](#_Toc508424378)

[OFAC | Reporting 32](#_Toc508424379)

[OFAC | Compliance Program & Risk Assessment 32](#_Toc508424380)

[Correspondent Accounts 33](#_Toc508424381)

[Bulk Shipments of Currency 34](#_Toc508424382)

[Electronic Banking 34](#_Toc508424383)

[Remote Deposit Capture 34](#_Toc508424384)

[ACH Transactions 34](#_Toc508424385)

[International ACH Payments 35](#_Toc508424386)

[Third Party Service Providers 35](#_Toc508424387)

[Prepaid Access 35](#_Toc508424388)

[Third Party Payment Processors 37](#_Toc508424389)

[Brokered Deposits 37](#_Toc508424390)

[Privately Owned ATMs 37](#_Toc508424391)

[Non-Deposit Investment Products and Insurance 38](#_Toc508424392)

[Concentration Accounts 38](#_Toc508424393)

[Custodial CDs 38](#_Toc508424394)

[Check Cashing for Non-Customers 38](#_Toc508424395)

[Lending Activities 39](#_Toc508424396)

[Trade Finance Activities 39](#_Toc508424397)

[Trust and Asset Management Services 39](#_Toc508424398)

[High Balance Customers 39](#_Toc508424399)

[Non-Resident Aliens and Foreign Individuals 39](#_Toc508424400)

[Politically Exposed Persons 40](#_Toc508424401)

[Non-Bank Financial Institutions and MSBs 40](#_Toc508424402)

[Professional Service Providers 41](#_Toc508424403)

[Non-Governmental Organizations and Charities 42](#_Toc508424404)

[Business Entities | Domestic and Foreign 42](#_Toc508424405)

[Cash Intensive Businesses 42](#_Toc508424406)

[Banking Marijuana-Related Businesses 43](#_Toc508424407)

[Ponzi & Other Schemes 43](#_Toc508424408)

[Elder Financial Exploitation 44](#_Toc508424409)

[BSA Recordkeeping Requirements 46](#_Toc508424410)

[Penalties for Non-Compliance 48](#_Toc508424411)

# Background and Policy Statement

[Insert Financial Institution Here] has established goal of maintaining a Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) compliance program with strong monitoring procedures in place. We have implemented a process by which we continuously identify and monitor the risks that could directly impact the quality of our BSA/AML compliance program. By analyzing and understanding our BSA/AML risk profile, we have been able to apply appropriate risk management processes to, and controls within, the BSA/AML compliance program to mitigate risk.

# Board Oversight

The Board of Directors is ultimately responsible for ensuring the bank maintains an effective BSA/AML program. As a result, management is required to develop policies and procedures designed to limit and reasonably control BSA/AML risks identified in the risk assessment. The Board is also responsible for designating a qualified BSA/AML Compliance Officer to oversee daily compliance. This designation must be made by formal Board resolution at least annually and noted within the minutes of the meeting in which the designation is made. The Board of Directors is responsible for ensuring that the BSA Officer has sufficient authority and resources to administer an effective BSA/AML Program based on the bank’s risk profile.

# BSA/AML Compliance Program Components

As required by law, our BSA/AML compliance program must be written, approved by the Board of Directors and noted in the Board minutes. We must have a BSA/AML compliance program that is commensurate with our risk profile. Our BSA/AML compliance program must be fully implemented and reasonably designed to meet BSA requirements. We acknowledge that policy statements alone are not sufficient; our practices must coincide with our written policies, procedures and processes. Our BSA/AML compliance program must provide for the following minimum requirements, also referred to as the “pillars” of BSA:

* A system of internal controls to ensure ongoing compliance.
* Independent testing of BSA/AML compliance.
* Designation of an individual or individuals responsible for managing BSA compliance (i.e. BSA Officer).
* Training for appropriate personnel.

Additionally, we must include a Customer Identification Program as part of our BSA/AML compliance program.

# BSA/AML Risk Assessment

We acknowledge the value in establishing a comprehensive risk assessment to aid us in applying appropriate risk management processes to, and controls within, our BSA/AML compliance program with the objective of mitigating that risk. We also acknowledge that the risk assessment process has helped us in identifying and mitigating gaps in our controls. In the 2Q2016, we undertook an initiative to overhaul the existing BSA/AML risk assessment to ensure that our resulting BSA/AML risk assessment is representative of our BSA/AML risk as presented by our operations, markets, customer base, products, services and risk management practices. Based on the information analyzed within our risk assessment, we have identified our BSA/AML risk profile to be moderate.

We also acknowledge that our risks will change as we implement new products and services, enter new markets, take on new customers and make changes operationally and strategically. As such, we have committed to maintaining a dynamic risk assessment that is proactively updated for any changes that could impact the bank’s risk profile.

# Internal Control Requirements

The Board, acting through Senior Management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. Internal controls are our policies, procedures and processes designed to limit and control risks and to achieve compliance with the BSA. The following table highlights internal control requirements and the actions we have taken to ensure we have implemented satisfactory controls. Internal controls should:

| [Insert Financial Institution Here] BSA/AML INTERNAL CONTROL STRUCTURE | |
| --- | --- |
|  | Identify banking operations more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the bank’s risk profile; and, provide for a BSA/AML compliance program tailored to manage risks. |
|  | Inform the Board, or appropriate subcommittee, and Senior Management of compliance initiatives, identified compliance deficiencies, and corrective actions taken, and notify directors and senior management of SARs filed. |
|  | Identify a person or persons responsible for BSA/AML compliance. |
|  | Provide for program continuity despite changes in management or employee composition or structure. |
|  | Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance and provide for timely updates in response to changes in regulations. |
|  | Implement risk-based CDD policies, procedures and processes. |
|  | Identify reportable transactions and accurately file all required reports including SARs, CTRs and CTR exemptions. |
|  | Provide for dual controls and the segregation of duties to the extent possible. |
|  | Provide sufficient controls and systems for filing CTRs and CTR exemptions. |
|  | Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity. |
|  | Provide for adequate supervision of employees that handle currency transactions, complete reports grant exemptions monitor for suspicious activity or engage in any other activity covered by the BSA and its implementing regulations. |
|  | Incorporate BSA compliance into the job descriptions and performance evaluations of bank personnel, as appropriate. |
|  | Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines. |

# Independent Testing Requirements

Under the pillars of BSA, we are required to ensure independent testing of the adequacy of our BSA/AML compliance program is conducted every 12-18 months. We acknowledge that our risk profile, driven by our products, services, customer base and markets, presents elevated BSA/AML risk and as such, it is the policy of [Insert Financial Institution Here] to engage an independent third party to conduct the bank’s BSA/AML audit every 12 months, at a minimum. It should be noted that two independent testing functions support one another in this endeavor: one audit assesses the adequacy of the bank’s BSA/AML compliance program over the “core” bank, while a second audit, performed by a separate independent third party, assesses the adequacy of our BSA/AML controls over the bank’s prepaid card function. The independent third parties performing such audits are subject to the bank’s vendor management process.

We have laid out the following, in accordance with regulatory guidance, as minimum requirements for our BSA/AML independent testing process:

| [Insert Financial Institution Here] BSA/AML INDEPENDENT TESTING REQUIREMENTS | |
| --- | --- |
|  | An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures and processes. We require an explicit statement about the BSA/AML compliance program’s overall effectiveness and compliance with applicable regulatory requirements. |
|  | A review of the bank’s risk assessment for reasonableness given our risk profile. |
|  | Appropriate risk-based transactional testing to verify our bank’s adherence to the 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. |
|  | A review of staff training for adequacy, accuracy and completeness. |
|  | A review of the effectiveness of our suspicious activity monitoring systems. |
|  | An assessment of our process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness and effectiveness of our policy. |
|  | An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program, including reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales and analytical and trend reports. |

We require that the audit scope, procedures performed, transactional testing completed and findings from the review be defined and documented. All audit documentation and work papers are available for examiner review.

Any violations, policy or procedure exceptions or other deficiencies are outlined within an audit report that is provided to the Board upon completion of the audit.

# BSA Officer Responsibilities

The Board recognizes its responsibility to designate a qualified individual to serve as our bank’s BSA Compliance Officer. The BSA Compliance Officer is responsible for coordinating and monitoring daily BSA/AML compliance. The BSA Officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank’s adherence to the BSA and its implementing regulations. The Board has designated a BSA Officer at the executive level who is responsible for daily oversight of the bank’s core and prepaid card BSA compliance programs. The BSA Officer is supported by an Assistant BSA Officer.

Both the BSA Officer and Assistant BSA Officer maintain certifications through the Association of Certified Anti-Money Laundering Specialists and are expected to fulfill continuing education requirements to maintain these certifications and remain knowledgeable of BSA/AML requirements, emerging risks, and areas of regulatory concern.

The BSA Officer must provide quarterly reports to the Board of Directors that address the following, at a minimum:

* Strengths and weaknesses within our BSA/AML program.
* Results of our most recent independent audit(s).
* Reports filed during the quarter.
* Changes in our bank’s risk profile, including recommendations for change and/or updates to our BSA/AML risk assessment or policy.
* Adequacy of resources, in terms of staffing, training and/or technology needs.

# Training Requirements

Ongoing and meaningful training is critical to effectively comply with the BSA and its supporting laws and regulations, as well as with our BSA/AML compliance program. On an annual basis, we provide for classroom-style BSA training for our staff during the bank’s all-employee in-service day. For this training, staff is divided into areas of responsibility and BSA training content is tailored to those groups. Senior Management also participates in these annual staff training sessions. As noted within this policy, the BSA Officer and Assistant BSA Officer are expected to fulfill continuing education requirements to maintain ACAMS certifications and to remain knowledgeable of BSA/AML requirements, emerging risks, and areas of regulatory concern. Resources have been allotted to ensure these requirements are met. The Board acknowledges that it must remain knowledgeable of BSA requirements and emerging issues. As such, resources have been dedicated to ensure the Board receives BSA compliance training annually, at a minimum.

[Insert Financial Institution Here]’s BSA/AML training initiatives are documented. Training and testing materials, dates of training sessions and attendance records are maintained by the bank’s Human Resources Officer and are available for examiner review.

The Money Laundering Process

In order to fully understand the purpose behind the practices and procedures incorporated in our BSA/AML compliance program, we must have an understanding of the money laundering process. Money laundering is the criminal practice of processing ill-gotten gains or “dirty” money, through a series of transactions. In this way, funds are “cleaned” so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involved three independent steps that can occur simultaneously.

* Placement: The first and most vulnerable stage of money laundering. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. Examples may include: dividing large amounts of currency into less conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a cancelled vacation or insurance policy, or purchasing a series of monetary instruments that are collected and then deposited into accounts at another location or financial institutions.
* Layering: Involved moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples may include: exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in or more financial institutions
* Integration: Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from recorded connection to the funds by providing a plausible explanation for the source of funds. Examples may include: the purchase and resale of real estate, investment securities, foreign trusts or other assets

Additionally, we must understanding indications and risks of terrorist financing. The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or to abstain from doing any specific act through the threat of violence. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. As such, money laundering is often a vital component on terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping and narcotics trafficking, have been found to be a major source of funding. Other observed activities involve smuggling, fraud, theft, robbery, identity theft and use of conflict diamonds as well as the improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

It is crucial that we also address and understand elder financial exploitation. We can play a critical role in addressing elder financial exploitation through our knowledge of our customers and their accounts. We may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. [Insert Financial Institution Here] Bank may also become aware of such scams through our direct interactions with our customers who are being financially exploited. If we observe possible elder abuse red flags, we must contact the BSA Officer. The BSA Officer is then required to review the circumstance of the situation and determine whether a SAR filing may be warranted.

Customer Identification Program Overview

We are required by law to have a written Customer Identification Program (CIP). Our CIP is intended to enable us to form a reasonable belief that we know the true identities of our customers. Our CIP must include account opening procedures that specify the identifying information we obtain from each customer. We must also include reasonable and practical risk-based procedures for verifying the identity of each customer.

Under the CIP rule, an “account” is a formal banking 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 another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping service or to provide cash management, custodian or trust services.

An account does not include:

* Products or services for which a formal banking relationship is not established with a person, such as check cashing, funds transfer or the sale of a check or money order.
* Any account that the bank acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger or assumption of liabilities.
* Account opened to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

The CIP rule applies to a “customer”. A customer is a person (an individual, corporation, partnership, trust, estate or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity and an individual who opens a new account for any entity that is not a legal person. A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.

# CIP | Documents Required for Individuals

At a minimum, we must obtain the following identifying information from each customer before opening an account:

* Name
* Date of birth
* Address
* Identification number

For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential street address of the next of kin or of another contact individual may be accepted.

For a non-U.S. person, one or more of the following must be obtained:

* TIN.
* Passport number and country of issuance.
* Alien identification card number.
* Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Identifying documents used to verify our customers’ identities must provide evidence of a customer’s nationality or residence and bear a photograph or similar safeguard. We must obtain an unexpired, photo ID (e.g. driver’s license, passport, state-issued photo ID, resident alien card).

# CIP | Documents Required for Businesses

At a minimum, we must obtain the following identifying information from each customer before opening an account:

* Name
* Address (principal place of business, local office or other physical location)
* Identification number (including Amish)

For a person other than an individual, such as a corporation, partnership or trust, we must 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.

# CIP | Non-Documentary Verification Methods

We are not required to use non-documentary methods to verify a customer’s identity. However, in cases in which a customer may not have documents to satisfy our documentary identification methods, we may utilize non-documentary methods to verify a customer’s identity. We may contact the customer; independently verify a 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; check references with other financial institutions; or, obtain a financial statement.

The following situations may occur in the normal course of business. Please note [Insert Financial Institution Here]’s procedure for addressing each situation. Note: e-Funds queries are made for all new customers. For loan accounts, credit reports are obtained for all new customers.

|  |  |
| --- | --- |
| SITUATIONS IN WHICH NON-DOCUMENTARY VERIFICATION METHODS MAY BE USED | |
| Description of Situation | [Insert Financial Institution Here] Procedure |
| An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard |  |
| We are not familiar with the documents presented |  |
| The account is opened without obtaining documents (e.g. we obtain required information from the customer with the intent to verify it) |  |
| The customer opens the account without appearing in person |  |
| We are otherwise presenting with circumstances that increase the risk that we will be unable to verify the true identity of a customer through documents |  |

For accounts opened online, we utilize e-Funds and/or a credit report to verify the customer’s identity. We then follow up with customer contact to verify that the information provided is accurate. For non-individuals, we obtain financial statements, business credit reports and perform customer contact.

# CIP | Additional Identification Procedures for Specific Customers

There are situations where we obtain information about individuals with authority or control over an account, including signatories, in order to verify a customer’s identity. This verification method applies only when we cannot verify the customer’s true identity through documentary or non-documentary methods. For example, we may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when we cannot otherwise satisfactorily identify the sole proprietor or the partnership.

We will obtain CIP information on signatories for new accounts opened by entities, and if the risk warrants, we will verify their identity using established verification methods.

For our Amish customers who do not maintain photo ID, we have established an alternative method to verify their identities. We will accept a letter from the community’s Bishop attesting to the identity of our Amish customer who is requesting to open an account with [Insert Financial Institution Here]. Please note that the Amish customer must provide a TIN at the time of account opening.

# CIP | Circumstances under which the Bank should Not Open an Account

When identification verification procedures do not result in a reasonable belief of the true identity of the customer, the account should not be opened.

# CIP | Exceptions

Excluded from the definition of customer (and therefore excluded from CIP) are federal regulated banks, banks regulated by a state bank regulator, governmental entities and publicly traded companies.

Instead of obtaining a TIN from a customer prior to opening an account, an account may be opened without a taxpayer identification number where the customer has applied for, but has not yet received a taxpayer identification number. Where this exception is utilized, a copy of the TIN application must be made and kept with the other account opening documentation. The account should be flagged for review to ensure that the TIN was received within a reasonable time. Generally, this time should not exceed 6-8 weeks from the time of account opening. During this timeframe, the customer may have use of the account. If the TIN has not been received within this time period, customer contact should be made to determine its status. If the TIN is not forthcoming after contacting the customer, or if the bank has received notification that a TIN will not be issued, the account must be closed.

# CIP | When the Bank Should File a SAR

When an account is declined or closed due to the inability to verify the customer’s identity, the BSA Officer must be contacted to determine whether a SAR should be filed. Similarly, the BSA Officer should be notified of any unusual or suspicious identification documents or behaviors (e.g. reluctance to provide required information) observed at the time of account opening to determine whether a SAR should be filed.

# CIP | Comparison with Government Lists

Our CIP must include procedures for determining whether a customer appears on any federal government list of known or suspected terrorists or terrorist organizations. We are contacted by the U.S. Treasury in consultation with the FDIC when a list is issued. At that time, we must compare customer names against the list within a reasonable time of account opening or earlier, if required by the government, and as must also follow any directives that accompany the list. As of the date of this policy, there are no designated government lists to verify specifically for CIP purposes. Customer comparisons to Office of Foreign Assets Control lists and 314(a) requests remain separate and distinct requirements.

# CIP | Providing Customer Notice

We must provide customers with adequate notice that we will request information to verify their identities. The notice must describe our identification requirements and we must provide the notice in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before an account is opened. The content of our CIP Notice has been provided as Exhibit A to this policy.

# CIP | Reliance on another Financial Institution

We are permitted to rely on another financial institution to perform some or all of the elements of the CIP as long as the following criteria are met:

* The relied-upon financial institution is subject to a rule implementing AML program requirements and is regulated by a federal functional regulator.
* The customer has an account or is opening an account at the bank and at the other functionally regulated institution.
* Reliance is reasonable under the circumstances.
* The other financial institution enters into a contract requiring it to certify annually to the bank that is has implemented its AML program and it will perform (or its agent will perform) the specified requirements of the bank’s CIP.

# CIP | Use of Third Parties

The CIP rule does not alter our authority to use a third party, such as an agent or service provider, to perform services on our behalf. We are permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as our agent in connection with ah loan, to verify the identity of our customer. We can also arrange for a third party to maintain our records. However, with any other responsibility performed by a third party, we are ultimately responsible for that third party’s compliance with our CIP requirements. This requirement contrasts with the reliance provision of the CIP rule that permits the relied-upon party to take responsibility.

Accounts may be opened by a third party, such a prepaid card program manager or IPI investment products. In these instances, photo ID must be obtained, reviewed and documented for individuals. Additional verification is performed through credit reports, e-Funds, or a telephone call. For non-individuals, third parties must obtain articles of incorporation, government issued business licenses, partnership agreements, trust agreements, or certificates of good standing.

# CIP | Record Retention

At a minimum, we must retain the identifying information (name, address, date of birth for an individual, TIN and any other information required by the CIP) obtained at account opening for a period of 5 years after an account is closed. For credit cards, the retention period if 5 years after the account closes or becomes dormant. We must also keep a description of the following for 5 years after the record was made:

* Any document that was relied upon to verify identity, noting the type of document, the identification number, the place of issuance and, if any, the date of issuance and expiration date.
* The method and results of any measures undertaken to verify identity.
* The results of any substantive discrepancy discovered when verifying identity.

# Customer Due Diligence

Our BSA/AML compliance program must include the adoption and implementation of comprehensive CDD policies, procedures and processes for all customers, particularly those who present higher risk for money laundering and terrorist financing. We must also include enhanced CDD for higher-risk customers and ongoing due diligence of our customer base. CDD policies, procedures and processes are critical because they can aid us in:

* Detecting and reporting unusual or suspicious transactions that potentially expose the bank to financial loss, increased expenses or reputational risk.
* Avoiding criminal exposure from persons who use or attempt to use the bank’s products and services for illicit purposes.
* Adhering to safe and sound banking practices.

# CDD | Identifying Beneficial Owners

In May 2016, FinCEN issued Customer Due Diligence Requirements for Financial Institutions. The final rule amends existing rules to explicitly reference key elements of customer due diligence and set forward minimum standards for CDD that are believed to be fundamental to an effective anti-money laundering program. The rule becomes effective on July 11, 2016 and its requirements must be implemented by May 11, 2018.

Under this rule, we must identify and verify the identity of beneficial owners of all legal entity customers at the time a new account is opened. We verify the identity of the individuals identified as beneficial owners – NOT his or her status as a beneficial owner. We are required to establish and maintain written policies and procedures reasonably designed to identify and verify the identities of beneficial owners of legal entity customers. FinCEN is NOT imposing a categorical retroactive requirement.

A beneficial owner ishe natural person (as opposed to another legal entity). To aid in the determination of who meets the definition of a beneficial owner, FinCEN has provided for a two-prong test. **Each prong is intended to be an independent test.**

In cases where an individual is both a 25% owner and meets the definition for control, that same individual could be identified as a beneficial owner under both prongs. You may also identify other individuals that technically fall outside the proposed definition of “beneficial owner” in accordance with your risk mitigation and customer due diligence practices.

Exclusions to the beneficial ownership rule include:

* Financial institutions regulated by a Federal functional regulator or a bank regulated by a State bank regulator
* A department or agency of the United States, of any State, or of any political subdivision of a State
* Any entity established under the laws of the United States, of any State, or of any political subdivision of any State, or under an interstate compact between two or more states, that exercises governmental authority on behalf of the U.S. or of any such State or political subdivision
* Any entity (other than a bank)) whose common stock or analogous equity interests are listed on the New York, American or NASDAQ stock exchanges
* Any entity organized under the laws of the United States or any State at least 51% of whose common stock or analogous equity interests are held in a listed entity.
* An issuer of a class of securities registered under Section 12 of the Securities Exchange Act of 1934 or that is required to file reports under Section 15(d) of that Act
* An investment company, as defined in Section 3 of the Investment Company Act of 1940, that is registered with the SEC under that Act
* An investment adviser, as defined in Section 2022(a)(11) of the Investment Advisors Act of 1940 that is registered with the SEC under that Act
* An exchange or clearing agency, as defined in Section 3 of the Securities Exchange Act of 1934 that is registered under Section 6 or 17A of that Act
* Any other entity registered with the SEC under the Securities and Exchange Act of 1934
* A registered entity, commodity pool operators, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, each as defined in Section 1a of the Commodity Exchange Act that is registered with the CFTC
* A public accounting firm registered under Section 102 of the Sarbanes-Oxley Act
* A bank holding company, as defined in Section 2 of the Bank Holding Company Act of 1956 or a savings or loan holding company as defined in Section 10(n) of the Home Owners’ Loan Act
* A pooled investment vehicle that is operated or advised by a financial institution excluded from the rule
* An insurance company that is regulated by a State
* A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
* A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution
* Non-excluded pooled investment vehicles
* Intermediated account relationships
* A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities *(As in the case of other legal entities lacking significant equity interests, financial institutions would be expected to collect beneficial ownership information under the control prong only)*
* Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620
* Non-profit entities whether or not tax exempt *(from the ownership prong).* For purposes of this provision, a non-profit corporation or similar entity would include, among others, charitable, non-profit, not-for-profit, non-stock, public benefit or similar corporations
* Accounts established for the purchase and financing of postage and for which payments are remitted directly by the financial institution to the provider of the postage products \*\*
* Commercial accounts to financial insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker \*\*
* Accounts to finance the purchase or lease of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of the equipment \*\*

\*\* The three exemptions directly above are subject to further limitations to mitigate the remaining limited money laundering risks associated with them. (Refer to Page 22 of the Final rule for details)

The CDD Rule requires us to obtain information about the beneficial owners of a legal entity from the individual seeking to open a new account on behalf of the legal entity customer. This individual could, but would not necessarily, be a beneficial owner. Please refer to the **Beneficial Ownership Account Opening Procedures** to guide you through the account opening process and the **Customer Identification Program Procedures** for information required to be obtained from each beneficial owner (i.e. CIP procedures for individuals) and acceptable documentary and non-documentary methods of verifying an individual’s identity.

We must use beneficial ownership information as we use other information we gather regarding customers, including compliance with OFAC-administered sanctions. As such, we must screen each beneficial owner against the OFAC list prior to account opening and/or disbursement of loan proceeds.

FinCEN does not expect the information obtained under the CDD Rule to add additional 314(a) requirements. The regulation implementing Section 314(a) does not require the reporting of beneficial ownership information associated with an account or transaction matching a named subject in a 314(a) request. We are required to search our records for accounts or transactions matching a named subject and report whether a match exists using the identifying information provided in the request. However, we have established as our policy, to include beneficial ownership in our investigation processes in addressing and responding to 314(a) requests [adjust this section if you policy is different].

# CDD | Determining a Customer’s Risk Rating

At the time of account opening, staff complete a workflow within our BSA software platform designed to address both CIP and CDD requirements. The workflow walks account opening personnel through questions about a customer’s occupation or nature of business, purpose of the account, sources of funds and wealth, ownership control, domicile, anticipated account activity and other critical information that helps us to form an understanding about the customer and his/her/its anticipated relationship (and associated risk) with [Insert Financial Institution Here].   
  
CDD | Responsibilities for Reviewing and Revising Customer Risk Ratings   
Customers rated High Risk at the time of account opening will be subject to an internal 60-day look-back to determine whether the high risk rating is appropriate given transaction activity conducted in the first three months of account opening. A standard form has been developed to facilitate this look-back and document the assessment process.

This form is also utilized to perform monitoring of High and Moderate Risk Customers (i.e. those who have been identified as High or Moderate Risk based on ongoing monitoring, transaction activity, nature of business, etc.).

Criteria used to quantify risk and define/drive risk ratings has been outlined on the Customer Risk Assessment form.

# CDD | Enhanced Due Diligence for Higher-Risk Customers

Customers who pose higher money laundering or terrorist financing risks present increased exposure to our bank. Enhanced due diligence (EDD) for higher risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces our reputation, compliance and transaction risks. Are noted above, customers that pose elevated risks (i.e. moderate and high risk customers) are subject to comprehensive periodic account reviews that are designed to ascertain whether transactions are reflective of the anticipated and “normal” activity for a given customer and whether there is any unusual or suspicious activity conducted during the timeframe reviewed. Additionally, all customers are subject to ongoing behavior-based monitoring parameters within our BSA software platform.

# CDD for Lending Relationships

Extensions of credit are incorporated into the bank’s behavior-based BSA monitoring system. [Insert bank process]

# CDD | High Risk Banking Functions

As part of our BSA/AML risk assessment process, we reviewed all of our banking functions to determine those that present elevated BSA/AML risk. The most prominent of such functions include online account opening and the prepaid card function. Please refer to [Insert Financial Institution Here]’s BSA/AML risk assessment for complete details.

# Suspicious Activity Reporting

We must have processes in place to identify, evaluate and report suspicious activity. Suspicious activity reports (SARs) must be filed for:

* Criminal violations involving insider abuse in any amount.
* Criminal violations aggregating to $5,000 or more when a suspect can be identified.
* Criminal violations aggregating to $25,000 or more regardless of a potential suspect.
* Transactions conducted or attempted by, at or through the bank and aggregating to $5,000 or more if you know, suspect or have reason to suspect that the transaction involves illegal activity, is designed to evade reporting requirements or has no apparent lawful purpose.

As SAR should also be filed when activity is inconsistent with an individual’s occupation, nature of business or does not reflect “normal” account activity.

**Mandatory SAR Reporting of Cyber-Events**[[1]](#footnote-1)

We are required to report a suspicious transaction conducted or attempted by, at or through the bank that involves or aggregates to $5,000 or more in funds or other assets. If we suspect, or have reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions.

In determining whether a cyber-event should be reported, we should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, we should consider in aggregate the funds and assets involved in or put at risk by the cyber event.

When we report a cyber-event through a SAR, we should include, to the extent possible:

* Description and magnitude of the event.
* Known or suspected time, location and characteristics or signatures of the event.
* Indicators of compromise.
* Relevant IP addresses and their timestamps.
* Device identifiers.
* Methodologies used.
* Other information we believe is relevant.

# SAR Filing Requirements

SARs must be filed no later than 30 calendar days from the date of initial detection. If no subject can be identified, the time period for filing is extended to 60 days. The time period to file a SAR starts when we, in the course of our review or as a result of other factors, reach the conclusion that we know or have reason to suspect that activity meets one or more definitions of suspicious activity. “Initial detection” should not necessarily be interpreted as meaning the moment a transaction is highlighted for review.

When a SAR is filed, we must review account activity for the subsequent 90 days following the filing to determine whether the suspicious activity has persisted. If suspicious activity has continued, we must file a SAR for continuous suspicious activity. FinCEN guidance allows for an expanded filing deadline for continuous suspicious activity. We may file SARs for continuous suspicious activity after a 90-day review, with the filing deadline being 120 days after the date of the previously related SAR.

For situations requiring immediate attention, in addition to filing a timely SAR, we must immediately notify, by telephone, an “appropriate law enforcement authority” and, as necessary, our primary regulator. For this initial notification, an appropriate law enforcement authority would generally be the local office of the IRS Criminal Investigation Unit or the FBI. Notifying law enforcement of a suspicious activity does not relieve us of our obligation to file a SAR.

# Suspicious Activity Reporting Safe Harbor

Federal law provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation regardless of whether such reports are filed pursuant to SAR instructions. Specifically, the law provides that a bank and its directors, officers, employees and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, “shall not be liable to any person under any law or regulation of the United States, any constitution, law or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of the such disclosure or any other person identified in the disclosure”. The safe harbor applies to SARs filed with the required reporting thresholds as well as SARs filed voluntarily on any activity below required thresholds.

# Systems to Identify, Research and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. Generally effective suspicious activity monitoring and reporting systems include 5 key components:

1. Identification or alert of unusual activity, which may include: employee identification, law enforcement inquiries other referrals and transaction and surveillance monitoring system output.
2. Managing alerts.
3. SAR decision-making.
4. SAR completion and filing.
5. Monitoring and SAR filing on continuous activity.

These components are interdependent. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance.

# Identification of Unusual Activity

We use multiple methods to identify potentially suspicious activity, including but not limited to activity identified by employees during daily operations, law enforcement inquiries, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring system output or any combination of these methods.

* **Employee Identification:** During the course of daily operations, employees may observe unusual or potentially suspicious transaction activity. [Insert Financial Institution Here] ensures bank staff receive BSA training annually, at a minimum, to ensure staff are knowledgeable of possible red flags] for suspicious activity. [Describe escalation process **Please refer to Appendix F of the FFIEC BSA/AML Examination Manual for examples of money laundering and terrorist financing “red flags”.**
* **Law Enforcement Inquiries and Requests:** We must maintain processes for identifying subjects of law enforcement requires, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects and filing, as appropriate, SARs related to those subject. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters and section 314(a) requests.

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the bank. However, a law enforcement inquiry may be relevant to our customer and account risk assessments. We should assess all the information we know about our customer, including the receipt of a law enforcement inquiry, in accordance with our BSA/AML compliance program. We should determine whether a SAR should be filed based on all customer information available.

# Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. We must be aware of all methods of identification and should ensure our suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification.

# SAR Decision-Making Process

After thorough research and analysis has been completed, findings are forwarded to [decision maker]. We have outlined the following escalation process from the point of initial detection to disposition of the investigation, as shown below. [Describe escalation process]

We document our decisions to file a SAR, including specific reasons for not filing a SAR as thorough documentation provides a record of or SAR decision-making process, including final decisions not to file a SAR. [Describe documentation and where it is maintained]

# SAR Filing on Continuous Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues out a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN guidance allows for an expanded filing deadline for continuous suspicious activity. We may file SARs for continuous suspicious activity after a 90-day review, with the filing deadline being 120 days after the date of the previously related SAR. However, we may file SARs on continuing activity earlier than the 120-dy deadline if we believe the activity warranted earlier review by law enforcement. This practice notifies law enforcement of the continuing nature of activity in aggregate. In addition, this practice reminds us that we should continue to review the suspicious activity to determine whether other actions may be appropriate (e.g. terminating the relationship with the customer who is the subject of the filing).

Law enforcement may have an interest in ensuring certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that we maintain a particular account, we must ask for a written request. The written request must indicate that the agency has requested that we maintain the account and the purpose and duration of the request. Ultimately, however, the decision to maintain or close an account is ours. As such, we have outlined the following escalation process for repeat SAR filings. [Describe escalation process]

# SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. [Describe process for SAR completion. Who is responsible for completing and filing SARs? Is there an internal check to ensure narratives are adequate and that SARs are filed within regulatory timeframes?]

# Notifying the Board of SAR Filings

We are required to notify the Board of Directors or an appropriate subcommittee, that SARs have been filed. However, the regulations do not mandate a particular notification format. We may, but are not required to, provide actual copies of SARs to the Board or a Board subcommittee. However, given the sensitivity of the information contained within SARs and liability for inadvertent or willing disclosure, we have opted to provide the Board summaries of SAR filings in general terms. [What is the timeframe for reporting SARs to the Board?]

# Closing an Account Due to Continuous Suspicious Activity

We may find it necessary to close an account due to continuing suspicious activity. Decisions to close an account due to ongoing continuous activity are subject to an escalation and decision-making process as outlined on the preceding pages.

Law enforcement may have an interest in ensuring certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that we maintain a particular account, we must ask for a written request. The written request must indicate that the agency has requested that we maintain the account and the purpose and duration of the request. Ultimately, however, the decision to maintain or close an account is ours.

It is the responsibility of the Security Officer, the BSA Officer and the CEO to determine when it is prudent to close an account due to continuous suspicious activity.

# Prohibition of SAR Disclosure

No bank, and no director, officer, employee or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, as confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent the information would reveal the existence of a SAR.

# Documentation of Circumstances in which SARs have been considered, but Not Filed

After reviewing facts and circumstances, we may determine that a SAR filing is not warranted for activity flagged as possibly suspicious. In these cases, documentation is retained to support our decision not to file a SAR. For each of these circumstances, we review the files 90 days after the decision not to file a SAR is made to determine whether possibly suspicious activity has continued.

# Suspicious Activity Reporting Record Retention

We must retain copies of SARs and supporting documentation for 5 years from the filing date. We must provide all documentation supporting the filing a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency.

# Currency Transaction Reporting

We must monitor for and report cash transactions in excess of $10,000 in one business day. Total cash in and cash out must be considered. However, ins and outs are not combined; they are totaled separately. Multiple transactions conducted on one business day will be aggregated to determine whether they exceed $10,000 and are therefore reportable. Transactions include: denomination exchanges, IRAs, deposits, withdrawals, loan payments, ATM transactions, purchases of CDs, exchanges, cash received for funds transfers, cash used to purchase monetary instruments, conversion of currency to prepaid access and transactions involving armored car services.

# Aggregation of Currency Transactions

Multiple currency transactional totaling more than $10,000 during any on business day are treated as a single transaction if we have knowledge that they are by or on behalf of the same person. [Describe aggregation process] In cases where multiple businesses share a common owner, the presumption is that separately incorporated entities are independent persons. The currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person. We must determine whether multiple businesses that share a common owner are being operated independently. If we determine that these businesses (or one or more of the businesses and the private accounts of the owner) are not operating separately or independently of one another or their common owner (e.g. the businesses are staffed by the same employees and are located at the same address, the bank accounts of one business are repeatedly used to pay the expenses of another business, or the business bank accounts are repeatedly used to pay the payroll expenses of the owner) we may determine that aggregating the businesses’ transactions is appropriate because the transactions were made on behalf of a single person.

If we determine that the businesses are independent, we should not aggregate separate transactions for these businesses.

# CTR Completion and Filing

CTRs must be filed no later than 15 days after the transaction.

# Currency Transaction Reporting Exemptions

The Money Laundering Suppression Act of 1994 established a two-phase exemption process. Under Phase I exemptions, transactions in currency by banks, governmental departments or agencies and listed public companies and their subsidiaries are exempt from reporting. Under Phase II exemptions, transactions in currency by smaller businesses that meet specific criteria may be exempted.

| **PHASE I EXEMPTIONS** | **PHASE II EXEMPTIONS** |
| --- | --- |
| * A bank, to the extent of its domestic operations * A federal, state or local government agency or department * Any entity exercising governmental authority within the U.S. * Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National Market Security on the NASDAQ Stock Exchange (with some exceptions) * Any subsidiary (other than a bank) of any listed entity that is organized under U.S. law and at least 51% of whose common stock or analogous equity interest is owned by the listed entity. | **Non-Listed Businesses**   * Has maintained a transaction account at your bank for at least two months * Frequently engages in transactions in currency with the bank in excess of $10,000 (5+ per year) * Is incorporated or organized under the law of the U.S. or a state, or is registered and is eligible to do business within the U.S. or a state   OR, prior to the passing of two months’ time, the bank undertakes a risk-based analysis of the customer that allows you to form and document that the customer has a legitimate business purpose for conducting frequent large currency transactions  **Payroll Customers**   * Defined solely with respect to withdrawals for payroll purposes from existing exemptible accounts and is a person who: has maintained a transaction account at the bank for at least 2 months, operates a firm that frequently withdraws more than $10,000 in order to pay its U.S. employees in currency and is incorporated or organized under the laws of the U.S. or a state, or is registered as and eligible to do business within the U.S. or a state.   OR, prior to the passing of two months’ time, the bank undertakes a risk-based analysis of the customer that allows you to form and document that the customer has a legitimate business purpose for conducting frequent large currency transactions |

We must file a one-time Designation of Exempt Person Report (DOEP) to exempt from currency transaction reporting:

* Each eligible listed companies or eligible subsidiaries.
* Phase II exemptions.

The report must be filed electronically through the BSA E-Filing System within 30 days after the first transaction in currency that the bank wishes to exempt. We do not need to file a DOEP Report for Phase I customers that are banks, federal, state or local governments, or entities exercising governmental authority.

The information supporting each designation of a Phase I-exempt listed public company/subsidiary and Phase II exempt person must be reviewed and verified by the bank at least annually. We must document the annual review and verify at least annually that the Phase II exemptions are monitored for suspicious transactions.

An ineligible business is defined as a business engaged primarily in one or more of the following activities:

* Serving as a financial institution or as agents for a financial institution of any type.
* Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment or mobile homes.
* Practicing law, accounting or medicine.
* Auctioning of goods.
* Chartering or operation of ships, buses or aircraft.
* Operating a pawn brokerage.
* Engaging in gaming of any kind.
* Engaging in investment advisory services or investment banking services.
* Operating a real estate brokerage.
* Operating in title insurance activities and real estate closings.
* Engaging in trade union activities.
* Engaging in any other activity that may, from time to time, be specified by FinCEN, such as a marijuana-related business.

A business that engages in multiple business activities may qualify for an exemption as a non-listed business as long as no more than 50% of its gross revenues per year are derived from one or more of the ineligible business activities listed above.

# Safe Harbor for Failure to File CTRs

CTR rules provide a safe harbor that a bank is not liable for the failure to file a CTR for a transaction in currency by an exempt person, unless the bank knowingly provides false or incomplete information or has reason to believe that the customer does not qualify as an exempt customers. In the absence of any specific knowledge or information indicating that a customer no longer meets the requirements of an exempt person, we are entitled to a safe harbor from civil penalties to the extent we continue to treat the customer has an exempt customer until the date of the customer’s annual review.

# CTR Exemption Record Retention

We must retain copies of CTRs for 5 years from the date of filing.

# Information Sharing under the USA PATRIOT Act

On September 26, 2002, final regulations implementing section 314 of the USA PATRIOT Act became effective. The regulations established procedures for information sharing to deter money laundering and terrorist activity. On February 5, 2010, FinCEN amended the regulations to allow state, local and certain foreign law enforcement agencies access to the information sharing program.

# Section 314(a) Information Sharing

A federal, state, local or foreign law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. Upon receiving a completed written certification from a law enforcement agency, FinCEN may require us to search our records to determine whether we maintain or have maintained accounts for, or have engaged in transactions with, any specified individual, entity or organization

When we receive an information request, we must conduct a one-time search of our records to identify accounts or transactions of a named suspect. Unless otherwise instructed by an information request, we must search our records for currency accounts, accounts maintained during the preceding 12 months and transactions conducted outside of an account by or on behalf of a named suspect during the preceding 6 months. We must search or records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request. [Who are the points of contact? What is the search process? How are searches documented?]

The contents of these requests are confidential and are subject to similar controls established to comply with section 501 of the Gramm-Leach-Bliley Act for the protection of customers’ non-public personal information.

# Section 314(b) Information Sharing

Section 314(b) encourages financial institutions and associations of financial institutions located in the U.S. to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability. To avail our bank to the statutory safe harbor from liability, we must notify FinCEN of our intent to engage in information sharing and communicate that we have established and will maintain adequate procedures to protect the security and confidentiality of information shared. A notice to share is effective for 1 year. [Insert Financial Institution Here] does not participate in information sharing practices under Section 314(b).

# Purchase and Sale of Monetary Instruments

Banks sell a variety of monetary instruments (e.g. bank checks or drafts, including foreign drafts, money orders, cashier’s checks and traveler’s checks) in exchange for currency. Purchasing these instruments in amounts of less than $10,000 is a common method used by money launderers to evade large currency transaction reporting requirements. Once converted from currency, criminals typically deposit these instruments in accounts with other banks to facilitate the movement of funds through the payment system. In many cases, the persons involved do not have an account with the bank from which the instruments are purchased. [Indicate whether MIs are sold to non-customers]

We must verify the identity of personal purchasing monetary instruments for currency in amounts between $3,000 and $10,000 inclusive and to maintain records of all such sales. Records must be retained for 5 years.

Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more must be treated as one purchase. Multiple purchases during one business day totaling $3,000 or more must be aggregated and treated as one purchase if the bank has knowledge that the purchases have occurred.

We may have a policy to require customers who are deposit accountholders and who want to purchase monetary instruments in amounts between $3,000 and $10,000 with currency to first deposit the currency into their deposit accounts. Nothing within the BSA or its implementing regulations prohibits a bank from instituting such a policy. However, FinCEN has taken the position that when a customer purchases a monetary instrument in amounts between $3,000 and $10,000 using currency that the customer first deposits into the customer’s account, the transaction is still subject to recordkeeping requirements. [Describe whether the bank requires that a customer deposits funds into an existing account in order to purchase a monetary instrument]

|  |  |
| --- | --- |
| **MONETARY INSTRUMENT RECORDKEEPING** | |
| **ACCOUNTHOLDERS** | **NON-CUSTOMERS** |
| * Name of the purchaser * Date of purchase * Types of instruments purchased * Serial numbers of each of the instruments purchased * Dollar amounts of each of the instruments purchased in currency * Specific identifying information, if applicable | * Name and address of the purchaser * Social security or alien identification number of the purchaser * Date of birth of the purchaser * Date of purchase * Types of instruments purchased * Serial numbers of each of the instruments purchased * Dollar amounts of each of the instruments purchased * Specific identifying information for verifying the purchaser’s identity  (e.g. state of issuance and number on driver’s license)   *Note: If the purchaser cannot provide the required information at the time of the transaction or through the bank’s own previously verified records, the transaction should be refused.* |

# Recordkeeping Requirements for Monetary Instrument Sales

We must verify the identity of personal purchasing monetary instruments for currency in amounts between $3,000 and $10,000 inclusive and to maintain records of all such sales. Records must be retained for 5 years.

# Funds Transfers

Funds transfer systems enable the instantaneous transfer of funds, including both domestic and cross-border transfers. Consequently, these systems can present and attractive method to disguise the source of funds derived from illegal activity. The BSA was amended by the Annunzio-Wylie Anti-Money Laundering Act of 1992 to authorize the U.S. Treasury and the Federal Reserve Board to prescribe regulations for domestic and international funds transfers.

For each payment order in the amount of $3,000 or more that a bank accepts as an originator, we must obtain and retain:

* The name and address of the originator.
* Amount of the payment order.
* Date of the payment order.
* Any payment instructions.
* Identity of the beneficiary’s institution.
* As many of the following items are received with the payment order:
  + Name and address of the beneficiary.
  + Account number of the beneficiary.
  + Any other specific identifier of the beneficiary.

If the originator is not a bank customer, we must collect and retain the information listed above as well as additional information depending on whether the order is made in person.

|  |  |
| --- | --- |
| **MADE IN PERSON** | **NOT MADE IN PERSON** |
| * Name and address of person placing the order * Type of identification reviewed * Number of the identification document * The person’s TIN or alien identification number, passport number, etc. | * Name and address of the person placing the order * The person’s TIN or alien identification number, passport number, etc. |

We must retain records of funds transfers of $3,000 or more for 5 years

**Travel Rule:** For funds transfers of $3,000 or more, you must include the following information in the order at the time the order is sent to the receiving financial institution:

* Name of the transmitter and if the payment was ordered from an account, the account number of the transmitter.
* Address of the transmitter.
* Amount of the transmittal order.
* Date of the transmittal order.
* Identity of the recipient’s financial institution.
* As many of the following as are received with the order:
  + Name and address of the recipient.
  + Account number of the recipient.
  + Any other specific identifier of the recipient.
* Either the name and address or the numerical identifier of the transmitter’s financial institution.

There are no recordkeeping requirements in the Travel Rule.

If we are receiving a funds transfer, you must retain a record of the payment order for any payment order of $3,000 or more. If the beneficiary is not an established customer of the bank, we must retain the following information for each payment order of $3,000 or more:

|  |  |
| --- | --- |
| **PROCEEDS DELIVERED IN PERSON** | **PROCEEDS NOT DELIVERED IN PERSON** |
| * Name and address * Type of document reviewed * Number of the identification document * The person’s TIN or alien identification number, passport number, etc. * If you have knowledge that the person receiving the proceeds is not the beneficiary, you must obtain and retain a record of the beneficiary’s name and address as well as the beneficiary’s identification. | * If the proceeds are not delivered in person, you must retain a copy of the check or other instrument used to effect the payment or you must record the information on the instrument. * Name and address of the person to whom it was sent |

# Funds Transfer Recordkeeping

**Funds Transfers of $3,000 or More**

Or recordkeeping requirements with respect to funds transfer vary based upon our role in the funds transfer transaction.

Records to Retain as an Originator:

* Name and address of originator
* Amount of the payment order
* Execution date of the payment order
* Any payment instruction received from the originator with the payment order
* Identity of the beneficiary’s bank
* As many of the following items as are receive with the order: name and address of the beneficiary, account number of the beneficiary, any other specific identifier of the beneficiary
* For each payment order that the bank accepts for an originator that is not an established customer of the bank, we must obtain additional information under 31 CFR 1020.410(a)(2)

Records to Retain as an Intermediary or Beneficiary Bank:

* We must retain a record of the payment order

For each payment order that the bank accepts for a beneficiary that is not an established customer of the bank, we must obtain additional information under 31 CFR 1020.410(a)(3)

# Foreign Correspondent Account Recordkeeping, Reporting & Due Diligence

Foreign correspondent accounts can be a gateway into the U.S. financial system. Banks are required to establish a due diligence program that includes appropriate, specific, risk-based and where necessary, enhanced policies, procedures and controls that are reasonably designed to enable us to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered or managed by our bank.

However, [Insert Financial Institution Here] does not maintain any foreign correspondent accounts.

# Private Banking

Private banking can be broadly defined as providing personalized financial services to wealthy clients. Section 312 of the USA PATRIOT Act added a subsection that requires each U.S. financial institution that establishes, maintains, administers or manages a private banking account in the U.S. for a non-U.S. person to take certain AML measures with respect to these accounts. For purposes of 31 CFR 1010.620, a “private banking account” is an account or any combination of accounts maintained at a bank that satisfies all three of the following criteria:

* Requires a minimum aggregate deposit of funds or other assets of not less than $1 million.
* Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account.
* Is assigned to, or is administered by, in whole or in part, an officer, employee or agent of a bank acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.

[Insert Financial Institution Here] does not maintain any private banking relationships as defined by regulatory guidance.

# Special Measures under the USA PATRIOT Act

Section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury to require domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Section 311 provides the Secretary of the Treasury with a range of options that can be adapted to target specific money laundering and terrorist financing concerns.

Orders and regulations implementing specific special measures taken under Section 311 are not static; they can be issued or rescinded over time as the Secretary of the Treasury determines that a subject jurisdiction, institution, class of transactions or type of account is no longer of primary money laundering concern. Our BSA Department maintains several resources that are designed to alert us to any special measures issued. Additionally, we review FinCEN’s website on a monthly basis for current information on final special measures.

# International Transportation of Currency or Monetary Instruments Reporting

Each person, including a bank, who physically transports, mails or ships currency or monetary instruments in excess of $10,000 at one time out of or into the U.S. (and each person who causes such transportation, mailing or shipment) must file a Report of International Transportation of Currency or Monetary Instruments (CMIR). A CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customers at the time of entry or departure from the U.S. When a person receives currency or monetary instruments in an amount exceeding $10,000 at one time that have been shipped from any place outside the U.S., a CMIR must be filed with the appropriate Bureau of Customs and Border Protection officer or with the commissioner of Customs within 15 days or receipt of the instruments, unless a report has already been filed. The report is to be completed by or on behalf of the person request transfer of the currency or monetary instruments.

Regardless of whether an exemption from filing a CMIR applies, we are not relieved of other monitoring and reporting obligations under the BSA. We must report the receipt or disbursement of currency in excess of $10,000 on a CTR.

As of June 2016, [Insert Financial Institution Here] has not had any transactions conducted through the bank or for its customers that would require a CMIR filing.

# Report of Foreign Bank and Financial Assets

Each person, including a bank, subject to U.S. jurisdiction with a financial interest in, or signature or other authority over, a bank, a securities or other financial account in a foreign country must electronically file a Report of Foreign Bank and Financial Accounts (FBAR) if the aggregate value of these financial accounts exceeds $10,000 at any time during the calendar year. An FBAR must be filed on or before June 30 of each calendar year for foreign financial accounts where the aggregate vale exceeded $10,000 at any time during the previous calendar year.

As of June 2016, [Insert Financial Institution Here] did not maintain any such accounts that require FBAR filings.

# OFAC

The Office of Foreign Assets Control, an office of the U.S. Treasury, administers and enforces economic trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers and those engages in certain activities, such as the proliferation of weapons of mass destruction or transnational organized crime. All U.S. persons, including U.S. banks, bank holding companies and non-bank subsidiaries, must compliance with OFAC’s regulations. In general, the regulations that OFAC administers require us to:

* Block accounts and other property of specified countries, entities and individuals.
* Prohibit or reject unlicensed trade and financial transactions with specified countries.

# OFAC | Blocked Transactions

We must block transactions that:

* Are by or on behalf of a blocked individual or entity;
* Are to go through a blocked entity; or,
* Are in connection with a transactions in which a blocked individual or entity has an interest.

For example, if we would receive instructions to make a funds transfers payment that falls into one of these categories, we would execute the payment order and place the funds into a blocked account. A payment order cannot be cancelled or amended after it is received by a U.S. bank in the absence of authorization by OFAC.

# OFAC | Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e. the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected. It is important to note that the OFAC regime specifying prohibitions against certain countries, entities and individuals is separate and distinct from the provision within the BSA’s CIP regulation that requires us to compare new accounts against government lists of known or suspected terrorists prior to account opening.

# OFAC | Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of particular sanctions programs or is other justified by U.S. national security or foreign policy objectives.

[Insert Financial Institution Here] does not maintain any licenses with OFAC.

# OFAC | Reporting

We must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30th concerning assets blocked (as of June 30th). We must keep an accurate and full record of each rejected transaction for at least 5 years after the date of the transaction.

As of June 2016, [Insert Financial Institution Here] has not identified any transactions that require blocking (or subsequent reporting) to OFAC.

# OFAC | Compliance Program & Risk Assessment

While not required by specific regulation, but a matter of sound banking practice and in order to mitigate the risk of non-compliance with OFAC requirements, we must maintain an OFAC compliance program that identifies higher risk areas, provides for appropriate internal controls for screening and reporting, establishes independent testing for compliance, designates a bank employee or employees responsible for OFAC compliance and creates a training program for appropriate personnel in all relevant areas of the bank.

[Insert Financial Institution Here]’s OFAC Compliance Program is comprised of the following:

* **Risk Assessment:** We have utilized the FFIEC Risk Assessment Matrix to determine our level of risk of doing business with any individual, entity or other party on the OFAC list. Based on this risk assessment, attached as Exhibit B to this policy, we have determined our level of risk to be Low.
* **Internal Controls:** We have implemented controls to ensure we do not do business with any individual, entity or other party on the OFAC list. All potential customers must be compared to the OFAC list prior to account opening. For incoming and outgoing wire transfers, the originator and beneficiary are screened against the OFAC list. The employee performing the OFAC check is required to mark the check box beside the originator and beneficiary and must initial the wire transfer form. If a confirmed positive match is detected for an outgoing wire, the wire should not be sent and BSA Officer must be notified. If a confirmed positive match is detected for an incoming wire, the funds must be frozen and the BSA Officer must be contacted.

Tellers are required to screen all non-customers against the OFAC list who initiate cash advances or for check cashing services equal to or greater than $1,000, including the sale of monetary instruments.

Our customer base is screened against the OFAC list on a daily basis. When the bank receives notification that the OFAC list has been updated, the updated list is imported into the bank’s system. When the report is complete, a full scan of the customer base is performed and possible matches are reviewed by the BSA Officer.

* **Independent Testing:** The scope of our BSA audit (both for the core bank and prepaid card function) incorporates an assessment of OFAC compliance.
* **Individual Responsible for OFAC Compliance:** The Board has designated individuals who are responsible for OFAC compliance, as outlined within the bank’s organizational chart. These individuals are responsible for ongoing oversight and administration of our OFAC compliance program.
* **Training:** OFAC compliance requirements are incorporated into bank-wide BSA training that is primarily accomplished through our annual all-employee in-service day. BSA training is also incorporated into Board compliance training.

# Correspondent Accounts

Banks maintain correspondent relationships at other domestic banks to provide certain services that can be performed more economically or efficiency because of the other bank’s size, expertise in a certain line of business or geographic location. Such services may include:

* **Deposit Accounts:** “Due from bank” accounts, which represent the bank’s primary operating account.
* **Funds Transfers:** A transfer of funds between banks may result from the collection of checks or other cash items, transfer and settlement of securities transactions, transfer of participating loan funds, purchase or sale of federal funds or processing of customer transactions.
* **Other services:** Services include processing loan participations, facilitating secondary market loan sales, performing data processing and payroll services and exchanging foreign currency.

Because domestic banks must follow the same regulatory guidelines, BSA/AML risk in domestic correspondent baking, including bankers’ banks are minimal in comparison to other types of financial services.

[Insert Financial Institution Here] does not maintain any foreign correspondent banking relationships.

# Bulk Shipments of Currency

Bulk shipments of currency entails the transportation of large volumes of U.S. or foreign bank notes. Bulk shipments of currency can be sent from sources either inside or outside the U.S. to a bank in the U.S. Shipments can also made from a bank in the U.S. to a recipient in a foreign jurisdiction. [Describe bank’s exposure to bulk shipments of currency]

# Electronic Banking

E-banking systems, which provide electronic delivery of banking products to customers, include ATM transactions; online account opening; internet banking transactions; and, telephone banking. [Insert Financial Institution Here] offers Internet banking (e.g. online banking, bill pay, electronic statements, mobile banking, telephone banking and debit cards). Mobile banking was introduced to customers in 2011, which allowed customers to access mobile banking via a mobile application; view account balances and activity; make transfers, schedule bill payments or delete a scheduled payment; and, find the nearest branch or ATM. In 2014, [Insert Financial Institution Here] introduced mobile deposit to allow customers to deposit checks from their smart phones using the mobile banking application. Limitations (e.g. per check limits, daily limits and revolving 30-day limit) were implemented. Each user must meet certain criteria to be approved to use the service, including length of time the deposit account has been opened, average deposit amounts, etc. Due to the risk of check fraud and duplicate items through mobile deposit, deposited and rejected items are reviewed daily by the bank’s data processing department.

We must ensure that our monitoring systems adequately capture transactions conducted electronically. We must be alert to anomalies in account behavior, such as velocity of funds in the account, or in the case of ATMs, the number of debit cards associated with an account.

# Remote Deposit Capture

Remote deposit capture (RDC) is a deposit transaction delivery system that has made check and monetary instrument processing (e.g. traveler’s checks or money orders) more efficient. In broad terms, RDC allows our customers to scan a check or monetary instrument and then transmit the scanned image to our bank. Scanning and transmission activities occur at remote locations. RDC may expose us to various risks, including money laundering, fraud and information security. Fraudulent, sequentially numbered or physically altered documents, particularly money orders and traveler’s checks, may be more difficult to detect when submitted by RDC and not inspected by a qualified person.

We have implemented the following controls over our RDC products: [Describe RDC controls]

# ACH Transactions

Traditionally, the ACH system has been used for the direct deposit of payroll and government benefit payments and for the direct payment of mortgages and loans. However, usage has expanded to include one-time debits and check conversation. Examples include credit payroll direct deposits, social security, dividends, interest payments, mortgage and other loan payments, insurance premiums and a variety of other consumer payments initiated through merchants or businesses. [Describe bank’s ACH exposure. Does the bank originate and receive?]

# International ACH Payments

The IAT is a Standard Entry Class code for ACH payments that enables us to identify and monitor international ACH payments and perform screening to ensure compliance with OFAC requirements. [Describe bank’s IAT exposure and processes]

# Third Party Service Providers

A third party service provider (TPSP) is an entity other than an originator, ODFI or RDFI that performs any functions on behalf of an originator, ODFI or RDFI with respect to the processing of ACH entries. The ACH system was designed to transfer a high volume of low-dollar domestic transactions, which pose lower BSA/AML risks. However, the ability to send out high-dollar and international transactions may expose us to higher BSA/Aml risks. ACH transactions that are originated through a TPSP may also increase BSA/AML risks, making it difficult for an IDFO to underwrite and review originator transactions for compliance with BSA/AML rules. Risks are heightened when neither the TPSP nor the ODFI performs due diligence on the companies for whom they are originating payments. [Describe the bank’s TSPS exposure and controls]

# Prepaid Access

[Insert Financial Institution Here] has established a growing prepaid access line of business that has increased the bank’s risk profile with regard to the size and complexity of the programs as well as regulatory scrutiny over administration of this line of business. Inherently, this line of business presents elevated levels of risk. Law enforcement investigations have found that some prepaid cardholders have used false identification and funded their initial loads with stolen credit cards, or have purchased multiple prepaid cards under aliases. In the placement phase of money laundering, criminals may load cash from illicit sources onto prepaid access products and send them to accomplices inside or outside the United States. Investigations have disclosed that both open- and closed-loop prepaid cards have been used in conjunction with, or as a replacement to, bulk cash smuggling. Transactions may pose the following unique risks to the bank:

* + 1. Funds may be transferred to or from an unknown third party.
    2. Verification of cardholder identity may be done entirely remotely, relying on third party program managers, processors or distributors.
    3. As with other modes of electronic payments, holders may be able to use prepaid access products internationally, thus avoiding border restrictions and reporting requirements applicable to cash and monetary instruments.
    4. Transactions may be credited or debited to the user’s payment product immediately, although there may be a lag in delivery of funds to the issuing bank, creating a load timing risk for the bank.
    5. Specific holder activity may be difficult to determine by reviewing activity through a pooled account.
    6. Data in underlying pooled accounts may be held or managed by third parties, separate from the issuing bank.
    7. Marketing of payment products, customer service and onboarding of new customers may be handled primarily by third parties separate from the issuing bank.
    8. The customer may perceive the transactions as less transparent.
    9. Source of payroll funding may come through an intermediary bank and may not be transparent.

To help mitigate BSA, fraud and other risks, as well as to address regulatory concern, [Insert Financial Institution Here] has implemented several controls within its prepaid access function. The bank created a Prepaid Card Program Committee, which has primary and ongoing oversight of the prepaid access function. Over the last twelve (12) months, the committee has developed a multi-layered oversight process. Detailed Fact Sheets were developed for each program. The data within these fact sheets was then used to create risk assessments for each program. Fact sheets and risk assessments provide consistency in program documentation and assessment. In 2016, these documents were expanded to include a cover sheet that provides a “snapshot” of each program.

The Committee has applied this process to new and existing programs. These documents and the resulting risk then flows through to the bank’s Global Prepaid Card Risk Assessment and Policy, which lay out the framework for program administration.

The bank relies on third-party program managers to employ identity verification processes to reasonably identify card applicants for programs that require KYC procedures. Management has established testing procedures to ensure these processes are being followed by program managers. Any CIP failures identified by the bank during testing are relayed back to the program manager for further information and possible blocking of cardholder funds until appropriate customer information is obtained.

Each program has predetermined load and balance caps as well as other thresholds. Activity is monitored on an ongoing basis and any activity outside the established thresholds is brought to the attention of program managers. Depending on the severity of the issue (i.e. dollar amount involved and/or frequency of attempts) the card may be closed and/or a suspicious activity report filed.

Representatives from the Prepaid Card Program Committee routinely communicate with program managers. The Committee meets on an ongoing basis via teleconference, with meeting typically held every other week. Meetings are conducted according to an established agenda and minutes of meeting discussions are formally documented.

Ongoing education has been identified as critical to ongoing effective administration of the bank’s prepaid card function. Each member of the committee has been assigned, and must successfully complete, training specifically designed for those involved in the prepaid industry. Additionally, the BSA and Assistant BSA Officers successfully completed coursework and testing under the Certified Anti-Money Laundering Specialist program sponsored by the Association of Certified Anti-Money Laundering Specialists (ACAMS).

Independent testing primarily focused on the bank’s prepaid access function has also been identified as a critical control. In 2015, [Insert Financial Institution Here] engaged a third party (Crowe) to perform a comprehensive audit of the bank’s prepaid card function. This audit resulted in the identification of several control and administrative weaknesses within the program. Management has incorporated these findings into the bank’s BSA Program Action Plan. Progress in addressing prepaid, as well as all BSA-related findings, is routinely monitored, discussed and documented.

# Third Party Payment Processors

Non-bank or third party payment processors are bank customers that provide payment-processing services to merchants and other business entities. These processors are not generally subject to BSA/AML requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes or other illicit transactions, including those prohibited by OFAC. [Describe bank’s exposure TPPPs]

# Brokered Deposits

The use of brokered deposits is a common funding source for many banks. Deposit brokers provide intermediary services for banks and investors. This activity is considered higher risk because each deposit broker operates under its own guidelines for obtaining deposits. Money laundering and terrorist financing risks arise because we may not know the ultimate beneficial owners or the sources of funds. The deposit broker could represent a range of clients that may be of higher risk for money laundering and terrorist financing.

[Insert Financial Institution Here] acquires brokered deposits through US Sterling and Depository Trust Company (DTC). US Sterling matches potential financial institution investors with an institution looking for brokered deposits. US Sterling is a federally regulated entity. CDs are opened in the names of client financial institutions. As such, the underlying financial institutions are exempt from CIP. However, [Insert Financial Institution Here] screens the institutions against the OFAC list when wire deposits are received.

DTC brokered CDs are opened with a tax ID number of DTC and all CDs are titled as CEDE and Co, in care of DTC.

US Sterling is registered with FINRA and maintains a BSA/AML compliance program that includes OFAC policies and procedures, all of which are on file at [Insert Financial Institution Here]. The procedures state that US Sterling is responsible for CIP, OFAC, FinCEN and Treasury recording and reporting. DTC is a member of the Federal Reserve. Brokered deposits from US Sterling and DTC are considered low risk due to their clients being financial institutions, which are federal regulated and therefore exempt from CIP requirements.

# Privately Owned ATMs

Privately owned ATMs are particularly susceptible to money laundering and fraud. Privately owned ATMs are typically found in convenience stores, bars, restaurants, grocery stores or check cashing establishments. Most dispense currency, but some dispense only a paper receipt (scrip) that the customer exchanges for goods or services. Fees and surcharges for withdrawals, coupled with additional business generated by customer access to an ATM, make the operation of a privately owned ATM profitable. Money laundering can occur through privately owned ATMs when an ATM is replenished with illicit currency that is subsequently withdrawn by legitimate customers. [What is the bank’s exposure to privately owned ATMs? What are the controls?]

The BSA software platform account opening workflow incorporates questions related to a potential customer’s operation of privately owned ATMs.

# Non-Deposit Investment Products and Insurance

We offer non-deposit investment products and insurance through a joint marketing arrangement IPI Financial. Under this relationship, [Insert Financial Institution Here] maintains a dual employee arrangement with IPI Financial whereby the bank’s NDIP and insurance professional is dually employed by the bank and IPI Financial. Because of this dual-employee arrangement, we retain responsibility over NDIP activities. [What is this arrangement? Per BSA guidance, even if contractual agreements establish the financial services corporation as being responsible for BSA/AML the bank needs to ensure proper oversight of its employees, including dual employees and their compliance with all regulatory requirements.]

# Concentration Accounts

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. Money laundering risk can arise in concentration accounts if the customer-identifying information, such as name, transaction amount and account number, is separated from the financial transaction. If separation occurs, the audit trail is lost and accounts may be misused or administered improperly. [Describe the usage and internal controls over concentration accounts]

# Custodial CDs

[Insert Financial Institution Here] maintains a custodial CD program. Due to the nature of these products, associated risk, as defined by regulatory guidance, is considered to be high. [Describe the controls over the custodial CD program. What is the monitoring process?]

# Check Cashing for Non-Customers

[Insert Financial Institution Here] will cash on-us checks for non-customers. Tellers, frontline personnel and customer service representatives must record all [Insert Financial Institution Here] checks cashed for non-customers when checks total $1,000 or more per item. The following information must be logged for each such transaction:

* The payee’s name.
* Date of transaction.
* Amount of the check presented.

Records must be maintained for 5 years. Employees are responsible for monitoring transactions for suspicious activity, such as unsigned checks, blank payees and structured transactions.

# Lending Activities

Lending activities include, but are not limited to, real estate, trade finance, cash-secured, credit card, consumer, commercial and agricultural. Lending activities can include multiple parties (e.g. guarantors, signatories, principals and loan participants). The involvement of multiple parties may increase the risk of money laundering or terrorist financing when the source of funds are not transparent. This lack of transparency can create opportunities in any of the three stages of money laundering or terrorist financing schemes. All loans are considered to be accounts for purposes of the CIP regulations. As such, we have implemented procedures to ensure all parties to loan transactions we originate are subject identity verification and OFAC screening prior to disbursement of loan proceeds. Additionally, we have implemented procedures by which lending transactions are monitored for suspicious activity on an ongoing basis. [Describe procedures]

# Trade Finance Activities

Trade finance typically involves short-term financing to facilitate the import and export of goods. These operations can involve payment if documentary requirements are met (i.e. letter of credit) or may instead involve payment if the original obligor defaults on the commercial terms of the transaction (e.g. guarantees or standby letters of credit). In both cases, a bank’s involvement in trade finance minimizes payment risk to importers and exporters. However, the international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection.

As of June 2016, [Insert Financial Institution Here] does not maintain any trade finance arrangements.

# Trust and Asset Management Services

Trust accounts are generally defined as a legal arrangement in which one party transfers ownership of assets to a person or bank to be held or used for the benefit of others. Trust and asset management accounts, including agency relationships, present BSA/AML concerns similar to those of deposit taking, lending and other traditional banking activities. Concerns are primarily due to the unique relationship structures involved when the bank handles trust and agency activities.

As of June 2016, [Insert Financial Institution Here] does not offer trust or asset management services.

# High Balance Customers

We run an internal report every 6 months to identify all customers or related and aggregated accounts with a minimum of $1 million on deposit. The report is reviewed for unusual fluctuations, ACH activity, cash transactions or transactions outside of the customer’s typical activity pattern.

# Non-Resident Aliens and Foreign Individuals

Foreign individuals maintaining relationships with U.S. banks can be divided into two categories: aliens and non-resident aliens (NRAs). For definitional purposes, an NRA is a non-U.S. citizen who: is not a lawful permanent resident of the U.S. during the calendar year and who does not meet the substantial presence test OR has not been issued an alien registration receipt card (i.e. Green Card). Although NRAs are not permanent residents, they may have a legitimate need to establish an account relationship with a U.S. bank. NRAs use bank products and services for asset preservation, business expansion and investments. It may be difficult to verify and authenticate an NRA accountholder’s identification, source of funds, and source of wealth, which may result in BSA/AML risks. We have implemented procedures to identify NRAs at the time of account opening and to ascertain the level of risk each NRA may present to our bank, based on factors such as:

* Accountholder’s home country.
* Types of products and services used.
* Forms of identification.
* Source of wealth and funds.
* Unusual account activity.

Risk levels are initially determined through completing the account opening workflow within our BSA software platform and are supported by ongoing behavior-based monitoring within the system.

When an NRA requests to open a deposit account, the account opening employee must notify the BSA Officer to ensure proper procedures are followed.

# Politically Exposed Persons

We must take reasonable steps to ensure that we do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior political figures (domestic and foreign), their families or their associates. Because the risks presented by PEPs vary by customer, product and service, country and industry, identifying, monitoring and designing controls for these accounts and transactions must be risk-based.

To determine whether an accountholder is a domestic or foreign senior political figure, we utilize the account opening workflow in our BSA software platform to ask relevant questions that would surface such association.

[Insert Financial Institution Here] maintains no account relationships with domestic or foreign senior political figures.

# Non-Bank Financial Institutions and MSBs

NBFIs are broadly defined as institutions other than banks that offer financial services. Common examples of NBFIs include, but are not limited to:

* Casinos and card clubs.
* Securities and commodities firms.
* Money service businesses.
* Insurance companies.
* Loan or finance companies.
* Operators of credit card systems.
* Other financial institutions (e.g. dealers in precious metals, stones or jewels; pawnbrokers).

NBFIs are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to their primary business (e.g. grocery store that offers check cashing). The range of products and services offered, and the customer bases served by NBFIs, are equally diverse. As a result of diversity, some NBFIs may be lower risk and some may be higher risk for money laundering.

To determine whether any existing or potential customer operates as an NBFI or MSB, we have built relevant questions into the our BSA software platform account opening workflow.

When an MSB is identified, we must follow specific procedures to ensure the MSB is appropriately registered with FinCEN as an MSB. We must also undertake the following actions to mitigate BSA/AML risk associated with MSB activities:

* Confirm the MSB is subject to examination for AML compliance by the IRS or state, as applicable.
* Affirm the existence of a written BSA/AML program and verify the BSA Officer’s name and contact information.
* Ensure the MSB’s established banking relations and/or account activity is consistent with expectations.
* Ensure the MSB is an established business with an operating history.
* Determine whether the MSB provides services only to local residents.
* Determine whether the MSB is a principal with one or a few agents, or its acting like an agent for one principal.
* Determine whether the MSB’s customers conduct routine transactions in low dollar amounts.
* Determine whether the MSB’s business operations are consistent with information obtained at the time of account opening.
* Determine whether money transmitting activities are limited to domestic entities or limited to lower dollar amounts.

As of June 2016, [Insert Financial Institution Here] does not maintain any account relationships with NBFIs or MSBs within the “core” bank. However, [Insert Financial Institution Here] has exposure to MSBs through or prepaid access/card program. To monitor these relationships and conduct ongoing monitoring, we have implemented an MSB risk assessment that is designed to determine the level of risk posed to the bank from these ongoing relationships.

# Professional Service Providers

A professional service provider (PSP) acts as an intermediary between its client and the bank. PSPs include lawyers, accountants, investment brokers and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client, or arrange for services to be performed on the client’s behalf, such as settlement of real estate transactions, asset transfers, management of client monies, investment services and trust arrangements. A typical example is interest on lawyers’ trust accounts (i.e. IOLTA). These accounts contain funds for a lawyer’s various clients and act as a standard bank account with one unique feature: The interest earned on the account is ceded to the state bank association or another entity for public interest and pro bono purposes.

In contrast to escrow accounts that are set up to serve individual clients, PSP accounts allow for ongoing business transactions with multiple clients. Generally, we have no direct relationship with or knowledge of the beneficial owners of these accounts, who may be a constantly changing group of individuals and legal entities.

Within our account opening workflow in our BSA software platform, we ask specific questions designed to determine whether a customer could be classified as a PSP. In rating the risk associated with any customer, including PSPs, our workflow takes into account risk factors, in addition to the nature of our customer’s business, to determine the level of BSA/AML risk exposure to our bank.

# Non-Governmental Organizations and Charities

Within our account opening workflow in our BSA software platform, we ask specific questions designed to determine whether a customer could be classified as an NGO or charity. In rating the risk associated with any customer, including NGOs and charities, our workflow takes into account risk factors, in addition to the nature of our customer’s business, to determine the level of BSA/AML risk exposure to our bank

# Business Entities | Domestic and Foreign

Within our account opening workflow in our BSA software platform, we ask specific questions designed to determine whether a customer could be classified as a domestic or foreign business entity. In rating the risk associated with any customer, including domestic and foreign business entities, our workflow takes into account risk factors, in addition to the nature of our customer’s business, to determine the level of BSA/AML risk exposure to our bank

As of June 2016, [Insert Financial Institution Here] does not maintain account relationships with any foreign business entities. Domestic business entities are subject to ongoing monitoring conducted through our BSA software platform. Accounts presenting moderate or high risk are subject to additional monitoring and review.

# Cash Intensive Businesses

Within our account opening workflow in our BSA software platform, we ask specific questions designed to determine whether a customer could be classified as a cash intensive business. In rating the risk associated with any customer, including cash intensive businesses, our workflow takes into account risk factors, in addition to the nature of our customer’s business, to determine the level of BSA/AML risk exposure to our bank

Cash intensive businesses are subject to ongoing monitoring conducted through our BSA software platform. Accounts presenting moderate or high risk are subject to additional monitoring and review.

# Banking Marijuana-Related Businesses

The Controlled Substances Act (CSA) makes it illegal under federal law to manufacture, distribute or dispense marijuana. Many states impose and enforce similar prohibition. Notwithstanding the federal ban, 29[[2]](#endnote-1) states and the District of Columbus have legalized the use of medical marijuana, while 6 states have also legalized the use of recreational marijuana. Because of the disconnect between federal and state laws concerning marijuana manufacture, distribution, dispensary and use, former United States Deputy Attorney General James M. Cole issued a memorandum (Cole Memo) to all U.S. Attorneys providing guidance to federal prosecutors concerning marijuana enforcement under the CSA. The Cole Memo guidance applied to all Department of Justice enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states.

However, in January 2018, U.S. Attorney General Jeff Sessions announced his decision to rescind this policy, allowing federal prosecutors to bring forth criminal cases against marijuana manufacturers and distributors. The decision to reverse policy, given the growth of the cannabis industry caused confusion among financial institutions about how to do business with marijuana manufacturers, distributors and dispensary without running afoul of federal money laundering laws.

While this policy outlines the provisions of the rescinded Cole Memo and discusses the bank’s required actions to be taken in banking marijuana manufacturers, distributors and dispensaries, it is the policy of [Insert Financial Institution Here] not to do business with identified marijuana-related businesses (MRBs) until resolution is achieved at the federal level. [You will want to adjust this paragraph, should you do business or plan to do business with MRBs at the state level].

Please refer to the Banking Marijuana Policy maintained under separate cover.

# Ponzi & Other Schemes

These types of schemes can offer consistent “profits” only as long as the number of investors continues to increase. The schemes are self-sustaining as long as cash outflows can be matched by monetary inflows. Ponzi schemes are based on fraudulent investment management services. Investors contribute money to the “portfolio manager” who promises them a high return and then when those investors want their money back, they are paid out with the incoming funds contributed by later investors. The individual organizing this fraud is in charge of controlling the entire operation. They merely transfer funds from one client to another and forgo any real investment activities.

We have trained our staff to look for and report the following red flags that could indicate possible Ponzi schemes:

* Customers who provide insufficient or suspicious information
* Customers who are reluctant to comply with reporting and recordkeeping requirements
* Funds transfers to or from a financial secrecy haven
* Unusual transfers of funds between related entities
* Sudden inconsistencies in currency transaction patterns
* Suspicious intracompany transfers and other banking activity by a company combined with establishment of a bank or a branch office in the company’s offices where, due to electronic connections between the bank and company’s systems, bank representatives could monitor all banking activity of the company
* Criminal history of a company’s principals combined with the company’s lack of legitimate business activities, irregular documentation, bank employee visits to discuss company’s business and majority of bank branch employees simultaneously working at the company
* Banking procedures that violated internal rules combined with personal or business ties between the bank and company such as overlapping Boards of Directors or bank employees who were relatives of the company’s principal
* Discovery by a bank of prior criminal history of a company principal, litigation accusing the company of wrongdoing or regulatory enforcement activity concerning the company
* Continued provision of banking services by bank or company even after bank conducted diligence on company’s operations and decided to liquidate bank’s own position in company’s investment funds
* Diversion of funds to accounts not listed in deposit instructions
* Diversion of funds to personal commodities trading accounts
* Attendance by bank representatives at investor meetings where misrepresentations of the bank’s role were made
* Institution of unusual systems by a bank necessary to ensure against repeated “bouncing” of checks by company.

Activity will monitored through the normal transaction monitoring procedures and will be investigated by the BSA Officer in accordance with our SAR decision-making processes.

# Elder Financial Exploitation

We can play a key role in addressing elder financial exploitation due to the nature of the client relationship. Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable

We have trained our staff to monitor for and report to the BSA Officer the following red flags that may indicate the existence of elder financial exploitation.

* Erratic or unusual banking transactions, or changes in banking patterns:
  + Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
  + Sudden Non-Sufficient Fund activity;
  + Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
  + Debit transactions that are inconsistent for the elder;
  + Uncharacteristic attempts to wire large sums of money;
  + Closing of CDs or accounts without regard to penalties.
* Interactions with customers or caregivers:
  + A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
  + The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
  + The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;
  + A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
  + The customer moves away from existing relationships and toward new associations with other "friends" or strangers;
  + The elderly individual's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;
  + The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103 (future 31 CFR Chapter X), if we know, suspect, or have reason to suspect that a 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 we know of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, we should file a Suspicious Activity Report, selecting the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term "elder financial exploitation" in the narrative portion of all relevant SARs filed. It is important to note that the potential victim of elder financial exploitation *should not be reported as the subject* of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Elder abuse, including financial exploitation, is generally reported and investigated at the local level, with Adult Protective Services, District Attorney's offices, sheriff's offices, and police departments taking key roles. We emphasize that filers should continue to report all forms of elder abuse according to institutional policies and the requirements of state and local laws and regulations, where applicable.

# BSA Recordkeeping Requirements

The BSA establishes recordkeeping requirements related to various types of records including: customer accounts (e.g. loan, deposits, etc.), BSA filing requirements, and records that document a bank’s compliance with the BSA. In general, the BSA requires that we maintain most records for at least 5 years. These records can be maintained in many forms, including original, microfilm, electronic, copy or a reproduction. Whatever the method, we must ensure that the records are accessible in a reasonable period of time.

The records related to the transactions discussed below must be retained for 5 years. However, as noted, the records related to the identity of a bank customer must be maintained for 5 years after the account is closed. Additionally, on a case-by-case basis, we may be ordered or requested to maintain some of these records for longer periods (e.g. by U.S. Treasury Department Order or law enforcement investigation).

| BSA RECORDKEEPING REQUIREMENTS |
| --- |
| **Extensions of Credit in Excess of $10,000 (Not Secured by Real Property)**  Our records must contain: Name of borrower, address of borrower, amount of credit extended, nature/purpose of the loan, and the date of the loan. |
| **International Transactions in Excess of $10,000**  A record of any request made or instructions received or given regarding a transfer of currency or other monetary instruments, checks, funds, investment securities or credit greater than $10,000 to or from any person, account or place outside the U.S. |
| **Signature Cards**  A record of each grant of signature authority over each deposit account. |
| **Account Statements**  A statement, ledger card, or other records on each deposit account showing each transaction in, or with respect to, that account. |
| **Checks in Excess of $100**  Each check, draft or money order drawn on the bank or issued and payable by it that is in excess of $100 |
| **Deposits in Excess of $100**  Each deposit slip or credit ticket reflecting a transaction in excess of $100 or the equivalent records for direct deposit or other funds transfer deposit transactions. The slip or the ticket must record the amount of any currency involved. |
| **Records to Reconstruct Demand Deposit Accounts**  Records prepared or received by the ban in the ordinary course of business, which would be needed to reconstruct a transaction account and to trace a check in excess of $100 deposited in a demand deposit account through its domestic processing system or to supply a description of a deposited check in excess of $100. |
| **Certificates of Deposit Purchased or Presented**  The record must contain: Name of customer (purchaser or presenter); address of customer; TIN; description of the CD; notation of the method of payment if purchased; and, the date of the transaction. |
| **Purchase or Monetary Instruments of $3,000 or More**  We must maintain a record of each bank check or draft, cashier’s check, money order or traveler’s check for $3,000 or more in currency. If the purchaser has a deposit account with the bank, the record must contain: Name of purchaser; date of purchase; type(s) of instruments purchased; amount in dollars of each of the instrument(s) purchased; and, serial number(s) of the instrument(s) purchased.  If the purchaser does not have a deposit account with the bank, the record must contain: Name of purchaser; address of purchaser; social security number of purchaser or alien identification number; date of birth of the purchaser; date of purchase; type(s) of instrument purchased; amount in dollars of each of the instrument(s) purchased; serial number(s) of the instrument(s) purchased; and, description of document or method used to verify the name and address of the purchaser (e.g. driver’s license state of issuance and number) |
| **Funds Transfers of $3,000 or More**  Or recordkeeping requirements with respect to funds transfer vary based upon our role in the funds transfer transaction.  Records to Retain as an Originator:   * Name and address of originator * Amount of the payment order * Execution date of the payment order * Any payment instruction received from the originator with the payment order * Identity of the beneficiary’s bank * As many of the following items as are receive with the order: name and address of the beneficiary, account number of the beneficiary, any other specific identifier of the beneficiary * For each payment order that the bank accepts for an originator that is not an established customer of the bank, we must obtain additional information under 31 CFR 1020.410(a)(2)   Records to Retain as an Intermediary or Beneficiary Bank:   * We must retain a record of the payment order * For each payment order that the bank accepts for a beneficiary that is not an established customer of the bank, we must obtain additional information under 31 CFR 1020.410(a)(3) |
| **Suspicious Activity Report and Supporting Documentation**  We must maintain a record of any SAR filed and the original or business record equivalent of any supporting documentation for a period of 5 years from the date of filing. |
| **Currency Transaction Report**  We must maintain a record of all CTRs for a period of 5 years from the date of filing. |
| **Designation of Exempt Person**  We must maintain a record of all designation of persons exempt from CTR reporting as filed with the Treasury for a period of 5 years from the designation date. |
| **Customer Identification Program**  We must maintain a record of all information we obtain under our procedures for implementing our Customer Identification Program. At a minimum, these records must include:   * All identifying information about a customer (e.g. name, date of birth, TIN and address) * A description of the document that we relied upon to verify the identity of the customer * A description of the non-documentary methods and results of any measures we took to verify the identity of the customer * A description of our resolution of any substantive discrepancy discovered when verifying the identifying information obtained.   We must retain the identifying information about a customer for a period of 5 years after the account is closed, or in the case of credit card accounts, 5 years after the account becomes closed or dormant.  We must retain the information relied on, methods used to verify identity and resolution of discrepancies for a period of 5 years after the record is made. |
| **Comprehensive Iran Sanctions, Accountability and Divestment Act**  We must retain a copy of any report filed with FinCEN and any supporting documenting, including the foreign bank certification or other responses to an inquiry, for a period of 5 years. |

# Penalties for Non-Compliance

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000. Any property involved in a transaction or traceable to the proceeds of a criminal activity, including property such as loan collateral, personal property or bank accounts, may be subject to forfeiture. Banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For example, the Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment and forfeiture actions. Additionally, we could risk losing our bank charter and bank employees could risk bring removed and barred from banking.

There are also criminal penalties for willful violations of the BSA and its implementing regulations and for structuring transactions to evade BSA reporting requirements. For example, a person, including a bank employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or 5 years in prison, or both. A person who commits such a violation while also violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or 10 years in prison, or both. A bank that violates certain BSA provisions or special measures, faces criminal penalties up to the greater of $1 million or twice the value of the transaction.

The federal banking agencies and FinCEN can bring civil money penalty actions for violations of the BSA. In addition to criminal and civil money penalty actions taken against them, individual may be removed from banking for a violation of AML laws.

All of these actions are publicly available.

Employee Attestation

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, certify that I have received and read [Insert Financial Institution Here]’s BSA Policy. As a condition of my employment with [Insert Financial Institution Here], I will comply with the requirements and provisions within this policy and its supporting procedures.

|  |  |
| --- | --- |
|  |  |
| *Employee Name (Printed)* | *Title & Department* |
|  |  |
|  |  |
| *Employee Signature* | *Date* |

EXHIBIT A | CIP Notice

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.

1. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005> [↑](#footnote-ref-1)
2. As of March 2018 [↑](#endnote-ref-1)