**ANTI-MONEY LAUNDERING**

**TABLE OF CONTENTS**

[Anti-Money Laundering/Know Your Customer Policy 2](#_Toc508019165)

[Introduction 2](#_Toc508019166)

[Objectives 2](#_Toc508019167)

[Know Your Customer Standards 5](#_Toc508019168)

[Prohibited Customers 5](#_Toc508019169)

[Customer Identification Program (CIP) 6](#_Toc508019170)

[New Account Review 9](#_Toc508019171)

[OFAC Screening/Comparison with Government Lists 9](#_Toc508019172)

[KYC Due Diligence Requirements 10](#_Toc508019173)

[Money Laundering Risk Ratings 12](#_Toc508019174)

Beneficial Ownership Rule……… [12](#_Toc508019174)

[Additional KYC Due Diligence Requirements for Certain Customers, Related Parties, and Accounts 14](#_Toc508019175)

[New High-Risk Customers 14](#_Toc508019176)

[Politically Exposed Persons 15](#_Toc508019177)

[Money Services Businesses 17](#_Toc508019178)

[Hedge Funds 18](#_Toc508019179)

[Onboarding of Peer-to-Peer Lending Companies 19](#_Toc508019180)

[Reliance on Others 19](#_Toc508019181)

[Ongoing Relationship/Customer/Account Activities 20](#_Toc508019182)

[Special Measures 24](#_Toc508019183)

[Information Sharing 24](#_Toc508019184)

[Subpoenas Received from Law Enforcement 25](#_Toc508019185)

[Currency Transaction Reporting and Exemptions 26](#_Toc508019186)

[Safe Harbor Provision 27](#_Toc508019187)

[Recordkeeping and Record Retention Requirements 27](#_Toc508019188)

[AML Training 29](#_Toc508019189)

[BSA/AML Compliance Officer 29](#_Toc508019190)

[BSA/AML Risk Assessment 30](#_Toc508019191)

[Independent Testing 30](#_Toc508019192)

[Board Reporting 30](#_Toc508019193)

[APPENDIX A 31](#_Toc508019194)

[APPENDIX B 33](#_Toc508019195)

[APPENDIX C 38](#_Toc508019196)

[APPENDIX D 43](#_Toc508019197)

[APPENDIX E 44](#_Toc508019198)

[APPENDIX F 46](#_Toc508019199)

[APPENDIX G 47](#_Toc508019200)

[APPENDIX H 50](#_Toc508019201)

[APPENDIX I 51](#_Toc508019202)

Anti-Money Laundering/Know Your Customer Policy

Introduction

This Policy establishes a set of minimum standards for identifying, accepting, documenting, and approving customers and maintaining customer relationships. It also identifies a set of money laundering risk ratings, and includes standards for performing account surveillance, and maintaining records.

Non-compliance with the requirements of this policy could seriously undermine the reputation of and public confidence in the Bank and could result in disciplinary actions against the Bank and its employees, including civil and criminal penalties and other sanctions.

The U.S. Congress enacted the Bank Secrecy Act in October 1970 to prevent banks and other financial service providers from being used as intermediaries to hide the transfer or deposit of money derived from criminal activity. Since its passage, Congress has amended the BSA a number of times to enhance law enforcement effectiveness. The reporting and recordkeeping requirements of the BSA regulations create a paper trail for law enforcement to investigate money laundering schemes and other illegal activities. This paper trail operates to deter illegal activity and provides a means to trace movements of money through the financial system.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) was signed into law by President Bush on October 26, 2001, and contains strong measures to prevent, detect, and prosecute terrorist financing and international money laundering. Title III of the USA PATRIOT Act is the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001. It includes provisions for fighting international money laundering and blocking terrorist access to the U.S. financial systems.

Objectives

The primary objective of this Policy is to help protect the good name and reputation of the Bank, and to secure its premises and systems against misuse as a vehicle for money laundering, terrorist financing, and other illegal activities. Specific objectives include the following:

* To ensure compliance with applicable U.S. and local anti-money laundering and anti-terrorist financing laws and regulations while protecting the financial privacy and relationship between the Bank and its customers
* To establish minimum standards needed to determine and verify the identity of new customers and any other relevant account parties, and to require the application of enhanced due diligence standards to those customers considered higher-risk as a matter of law or regulations, or based upon the Bank’s own assessment of risk
* To set appropriate standards for the ongoing conduct of customer relationships
* To institute sound account/transaction surveillance standards as a mechanism for enabling Bank personnel to recognize, detect, and report money laundering, terrorist financing, and/or suspicious activity occurring through Bank accounts
* To delineate the responsibilities of employees who implement the Bank’s AML processes.

Policy

The Bank will comply with the U.S. Bank Secrecy Act (BSA), the USA PATRIOT Act, and other applicable AML laws and regulations. Also the Bank, consistent with applicable law, cooperates with governmental and law enforcement authorities in the enforcement of AML laws and regulations in connection with transactions involving the Bank.

No director, officer or employee of the Company shall:

* Knowingly engage in, or assist any other person or entity in engaging in, any activity believed by such director, officer or employee to involve money laundering, terrorist financing or other suspicious or criminal activity
* Assist any customer in structuring financial transactions in order to avoid disclosure to governmental or law enforcement authorities under applicable law
* Advise any customer that their information has been, or will be, reported to governmental or law enforcement authorities (unless informing the customer is permissible, such as during the preparation of a Currency Transaction Report)
* Make a conscious decision to avoid learning the truth about a customer’s suspected illegal activities.

Any director, officer or employee of the Company who fails to adhere to any of the foregoing policies may be subject to immediate demotion, reassignment or dismissal, and such failure may cause such individual and the Bank to be subject to severe civil and/or criminal penalties.

Money Laundering and Terrorist Financing

Money Laundering is the involvement in any one transaction, or series of transactions, which assists a person in keeping, concealing or disposing of the proceeds derived from illegal activities. It is the criminal act of processing “dirty” money, through a series of transactions; in this way the funds are “cleaned” so that they appear to be proceeds from legal activities.

***Refer to Appendix A for examples of suspicious conduct and transactions related to money laundering***

Although money laundering is a complex process, it basically involves the following three steps that can occur independently or simultaneously:

* The first stage of laundering money is placement. 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 an amount to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include dividing large amounts of currency such as purchasing a series of monetary instruments.
* The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions, to create confusion. Examples of layering include wiring funds to and through numerous accounts at many institutions.
* The final stage of the process is integration. Once the funds are in the financial system and obstructed through the layering stage, the integration stage is used to further create the appearance of legal funds through additional transactions. Examples include the real estate transactions or investment securities.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and drug trafficking, have been found to be a major source of funding. Other observed activities include improper use of charitable or relief funds that donors may have no knowledge that their donations have been diverted to support terrorist causes. Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate sources are a key difference between terrorist financiers and traditional criminal organizations.

Prohibited Countries

The Bank may determine that it will not process transactions involving certain countries, or maintain or open new accounts for clients located in certain countries, because of publicly reported concerns of law enforcement agencies and regulators with respect to money laundering controls in those countries. As events change, the Bank may add or delete countries from this prohibition.

***Refer to Appendix B for Countries Tiering List*** *.*

## Know Your Customer Standards

Sound business practices include the concept of knowing your customer. Observing the standards within this Policy can greatly reduce the risk that the Bank might be used for unlawful purposes. A sound Know Your Customer Policy include, at a minimum:

* Establishing the true identity of the customer and other related parties to the account, as appropriate
* Screening customer and, as appropriate, related party names against government lists
* Obtaining additional information/documentation as needed to understand the customer’s level of risk, determine the need for enhanced due diligence, and enable the detection of suspicious activity
* Determining the customer source of funds
* Understanding and recording the account’s purpose and anticipated transaction behavior
* Maintaining up-to-date knowledge of the customer through ongoing client contact and periodic reviews.

Prohibited Customers

The Bank intends to do business with reputable customers whose identity can be verified. The Bank will not knowingly do business with persons or entities with whom the Bank is prohibited from doing business because they are sanctioned under the U.S. Embargo Programs or any other official government lists that are identified and distributed throughout the Bank or are applicable in the local jurisdiction. Also those with whom the Company has chosen not to do business based on prior experience. In addition, Shell Banks which is one that does not have a physical presence in any country. Physical presence is defined as a place of business that (1) is maintained by a non-U.S. bank; (2) is located at a fixed address in a country in which the non-U.S. bank is authorized to conduct banking activities, at which location the non-U.S. bank employs one or more individuals on a full-time basis and maintains operating records related to its banking activities; and (3) is subject to inspection by the banking authority that licensed the non-U.S. bank to conduct banking activities.

Also, the Bank will not knowingly do business with individuals or entities:

* Whose character or financial conduct are suspect at the inception of the relationship or becomes suspect at any time during the relationship
* Convicted of money laundering or related financial crime
* Who attempt to establish anonymous accounts, accounts in obviously fictitious names or accounts where the identity of the true beneficial owner of the funds is required but cannot be obtained
* Who refuse to provide information required by the Bank

Customer Identification Program (CIP)

Minimum identifying information must be obtained, recorded and verified for any new customer prior to opening their first account or providing their first product/service. For the purpose of CIP requirements, a customer is defined as any person, including both individuals and entities (e.g., corporations, partnerships and trusts), that opens a new account, product or service, including deposit, transaction, asset, securities, safekeeping, collateral, or mutual fund accounts, credit, lending or borrowing activities, a safe deposit box, or cash management, custody, trust or estate services. Typically, the customer is the accountholder. In cases where an individual opens an account on behalf of a person who lacks legal capacity, such as a minor or an entity that is not a legal person, the individual opening the account is the customer. The following entities are excluded from the definition of customer for CIP purposes:

* Financial institutions regulated by a U.S. Federal functional regulator or banks regulated by a U.S. state bank regulator
* Departments or agencies of the U.S., including any state or political subdivision of any state
* Entities established under the laws of the U.S., state laws, political subdivision of any state, or under an interstate compact, that exercise governmental authority on behalf of the U.S., or any such State or political subdivision
* Publicly listed entities whose common stock or similar equity interests are listed on the New York Stock Exchange, the American Stock Exchange, or the NASDAQ Stock Market.

For new customers who are individuals, including joint accountholders, the following identification information must be obtained and recorded:

* Name
* Date of birth
* Primary residence address (and mailing address, if different from residence address). For a customer who does not have a residential or mailing address, a business street address, an Army Post Office or Fleet Post Office box number or the residential or business address of next of kin or of another contact individual
* Government issued identification number – For U.S. individuals, this number must be the Social Security Number. For non-U.S. individuals/foreign based individuals, the number can be a taxpayer identification number, passport number, national identification number, resident’s identification number, alien identification number, or another government-issued identification number.

For new customers who are entities, the following identification information must be obtained and recorded:

* Legal name
* Principal place of business address (or local office address)
* Government issued identification number – For U.S. entities (established or organized in the U.S.), this number must be the Taxpayer Identification Number (TIN/Employer Identification Number (EIN). For non-U.S. entities/foreign based individuals, this number can be a taxpayer identification number, registration number, or another government-issued identification number. Alternative government-issued documentation that certifies existence must be requested for any non-U.S. entities that do not have an identification number.

There may be instances (i.e., a newly formed entity) when the customer has applied for the TIN/EIN, but it has not been received at the time the account is requested. In all cases, the TIN/EIN must be obtained by the Bank within 60 days or the account must be closed. The Bank will track accounts opened without TINs/EINs, and may consider restricting account usage, such as limiting deposits, withdrawals, check writing, extension of credit or other measures while receipt of the TIN/EIN is pending.

The identification of each customer is typically verified before or at account opening. For all businesses, verification must be accomplished no later than 30 days after account opening. Identity verification can be accomplished through documentary or non-documentary means or a combination of both. Depending on the risks associated with the customer, businesses may consider whether to restrict the customer’s activities until such time that the verification has been completed.

Documentary verification is accomplished by obtaining, reviewing, and making a record of one acceptable form of identification document. For individual customers, acceptable identification documents include unexpired, government-issued photo IDs, such as:

* Passport
* Driver’s license or non-driver photo ID card
* Military ID card

For businesses/entities, acceptable identification documents include:

* Certificate of Incorporation/Filing Receipt
* General or Limited Partnership Agreement
* Articles of Organization or Association/Certification of Formation
* Trust Instrument
* Letters of Trusteeship or Executorship
* U.S. Internal Revenue Code Sec. 501(c)(3) letter (for nonprofit organizations)
* A government-issued business license
* For foreign based entities, those legal documents issued by other countries that parallel the above and authenticate the entity will be accepted upon verification.

These documents are to be used to confirm the accuracy of the information provided by new customers. A record of the document(s) used must be retained on file and should include: a description (i.e., the type of document), its identification number, the place of issuance, the date of issuance, and the expiration date (as applicable). A photocopy of the document (should the business choose to make and retain photocopies) will satisfy this requirement.

***Refer to Appendix C for further description of documentary verification documents***

The Bank may choose to perform non-documentary verification in addition to, or instead of, placing reliance on the documents named above. Non-documentary verification may include, but is not limited to:

* Contacting the customer at home after the relationship has been established
* Obtaining references from reliable sources (e.g., credit bureaus, other financial institutions)
* Performing a site visit at the entity customer’s place of business.

Even when not required, non-documentary verification may be considered an additional safeguard, particularly in higher-risk businesses and with high-risk customers. When non-documentary verification is used, a record must be made and retained of the methods undertaken to verify the identity of a customer; this record should include a description of the methods and the results of verification performed.

During the course of verifying the identity of a customer, discrepancies may arise between the information obtained from the customer and the information obtained during the verification. Resolutions resulting in the continuing the relationship need to be further documented and approved by a Vice President or above.

Bank employees are under no obligation to continue the customer identification and verification process if, at any time during this process, they determine that it is in the best interest of the Bank to terminate the relationship or discontinue the customer acceptance process. If the decision to discontinue customer acceptance is based on a CIP failure and is deemed suspicious, an Incident Report Form must be filed even though accounts are not opened.

The USA PATRIOT Act requires that, prior to opening an account that the Bank notify its customers that it will be requesting information to verify their identity. The Bank’s signage/brochure will include the following language:

**Important Information About Procedures For Opening a New Account**

*To help the government fight the funding of terrorism and money laundering activities, financial institutions are required by Federal law to obtain, verify, and record information that identifies each individual or entity that opens an account or requests credit.*

*What this means for individuals: When an individual opens an account or requests credit, we will ask for their name, residence address, date of birth, tax identification number, and other information that allows us to identify them. We may also ask to see a driver’s license, passport or other identifying documents.*

New Account Review

Within five business days, the branch manager or designee will review new account information and supporting documentation to determine whether all the necessary information was obtained, the account appears suspicious in any manner, the risk rating is proper and the type of account/business/customer is in compliance with bank policy. Also as part of this review, the branch manager or designee validates the information on the Insight system to ensure accuracy. The branch manager or designee signs the “Account Opening Data Entry Form” as evidence of the review and approval.

OFAC Screening/Comparison with Government Lists

Upon opening an account, the related party names are screened against the Office of Foreign Assets Control (OFAC) sanction list. Upon receipt of an update of the OFAC sanction list, the entire portfolio is scanned against this sanction list. Possible matches are investigated and any true matches are escalated to the OFAC Compliance Officer for resolution.

The new account will also be scanned to determine whether the customer appears on any list, should one be issued, of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. Possible matches are investigated and any true matches are escalated to the BSA/AML Compliance Officer. The BSA/AML Compliance Officer is responsible to ensure that all federal directives issued in connection with these lists are followed.

KYC Due Diligence Requirements

KYC due diligence must be performed on all new customers at the time the relationship with the Bank is first established.

For the purposes of KYC, the customer is each person in whose name an account is opened or a product/service is initiated. This person can be an individual, a company, an organization or other entity. The Bank will obtain information and perform due diligence on related parties where appropriate. Related parties include persons who have authority, or who are in a position of control, over the account, product or service, as well as the beneficial owner(s) of the assets and persons who are intended to receive a benefit from, or be a recipient under, the relationship. The following are some examples of related parties:

* The account’s nominal and/or beneficial owner(s)
* For an account in the name of an agent, the principal
* For a company account, the significant owners, principal officers, key senior managers, and directors of the company
* For an account in the name of a trust, the donor, trustees, and executors.

When opening a new account for an existing customer, it is not necessary to re-perform customer identification/verification steps provided that the existing customer information is current and complete and the Bank maintains the reasonable belief that it knows the true identity of the customer. Additional account level data, however, may be needed in certain circumstances relative to any additional accounts offered to existing customers. Similar account level data may also be necessary when a new account is opened for a new customer. Depending on the type of account, such additional information may include, but is not limited to:

* Type and purpose of account
* Source of initial and ongoing funding
* Anticipated activity: the anticipated usage, activity, types of transactions, volumes and dollar amounts

Beneficial Ownership Rule:

CRB staff is required to identify the beneficial owners of their legal entity customers-including corporations, limited liability companies, partnerships, business trusts, any other entity created by a filing with a state office, any similar entities formed under the laws of a non-US jurisdiction and similar entities-that open new accounts.

The definition of “legal entity customer” does not include:

* Natural persons
* Sole Proprietorships
* Unincorporated Associations (i.e. Boy Scouts, Girl Scouts, neighborhood associations)
* Trusts, other than statutory trusts created by a filing with a state office

Specifically, CRB must identify and verify Beneficial owners defined as:

1. one or more natural persons, if any, who directly or indirectly own 25% or more of a legal entity customer, through any contract, arrangement, understanding, relationship or otherwise, and;
2. a natural person who "controls" the entity with significant responsibility to control, manage, or direct a legal entity customer, including:

* An executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer);
* or any other individual who regularly performs similar functions.

Certain legal entities, including the following, are excluded from the Beneficial Ownership Rule:

* Domestic banks in the United States (including domestic offices of foreign banks);
* Entities listed on the New York, American, or NASDAQ stock exchanges;
* Majority-owned subsidiaries of such listed entities;
* Security issuers registered under Section 12 of the Securities Exchange Act of 1934;
* Investment companies;
* SEC- and CFTC- registered entities;
* Bank holding companies;
* Pooled investment vehicles operated by an entity that is not a legal entity customer;
* State-regulated insurance companies;
* Designated financial market utilities;
* Foreign financial institutions whose regulator maintains beneficial ownership information;
* Foreign government entities that do not engage in commercial activities; and
* Legal entities only to the extent that they open a private bank account

*Internal Account Requests:* The following policies apply when a bank employee submits an account opening request to the branch manager.

* The person submitting the form (i.e. the person signing the “Requested by” field) to the branch manager will be the Relationship Owner of the account.
* The Relationship Owner will be responsible for completing the following:
  + Gathering and ensuring that all information is complete to support the opening of the account;
  + Determining the money laundering risk rating
  + Any updating of Know Your Customer (KYC) information.  The Relationship Owner updates the KYC information, when there is a significant change in customer activity (for example new products added, or increase in transaction volume), ownership, or public information about the customer.
  + Completing the periodic review - For high risk customers, the periodic review occurs one per year, whereas for medium risk customers, the periodic review occurs once every two years (based on the date the account was opened).
  + Conducting site visits of high risk customers, in case there is a triggering event. Triggering events include: negative news; unusual increase/decrease in account activity; changes in the nature of the account activity; money laundering alerts that cannot be cleared; word of mouth tips; or reluctance from customer to provide information.

***Refer to Appendix D for a sample of the Internal New Account Request form***

Money Laundering Risk Ratings

Money laundering risk ratings are an evaluation of the customer’s/account’s potential money laundering risk. As such, they can impact the approvals needed to accept a customer or open the account, determine the extent of information and verification required, trigger the need for enhanced due diligence, and affect the frequency of periodic relationship reviews.

The relationship owner determines the money laundering risk rating but will be reviewed by another individual. Money laundering risk ratings must be determined before a new customer is accepted, and at, or immediately after, a new account is opened. They are to be re-evaluated and adjusted, as appropriate, during the periodic review process, or at any other time when the business learns of new information that affects the rating. The branch manager is responsible for reviewing or approving changes to a client’s risk rating.

Money laundering risk ratings apply at both the customer and account level. If a customer is high-risk by himself, because for example he is a politically exposed person or associated with a high-risk industry, then all of his accounts should be classified as high-risk. If an account is rated high-risk, however, the associated customer is not automatically high-risk.

Risk determination is a two-part process. First, the relationship owner must identify and understand the general operating and overall legal, regulatory and geopolitical environments in which their customers operate. Second, the relationship owner must, at a minimum, understand the following to determine whether they want to enter into, or sustain, a relationship with a particular customer within their target market:

* The nature of the customer, including their reputation and business or other financial activities
* The products and services requested, and the customer’s purpose for and use of such products and services
* The money laundering risks associated with the customer and the jurisdiction(s) with which the customer has significant contact.

Also the following risk factors will be considered:

* Customer-Type – At a minimum, the following customers shall be considered high-risk: Politically Exposed Persons, Money Services Businesses, Offshore International Business Corporations and Private Investment Companies, any customers associated with substantial negative public information.
* Geography – At a minimum, customers associated with (i.e., located/domiciled in, a citizen or resident of, and/or has business activities in) a Tier 1 country shall be considered high-risk. ***Refer to Appendix B for the Country Tiering List***
* Industry – At a minimum, customers associated with (i.e., one is principally engaged in or whose source of wealth was generated from) a high-risk industry shall be considered high-risk. ***Refer to Appendix E for the High- and Medium-Risk Industries List***
* Products and Services – At a minimum, customers and/or accounts that use high-risk products or services shall be considered high-risk. ***Refer to Appendix F for the Medium Risk Products List***
* Transaction Activity – Such as whether the customer’s expected transaction activity, including cash and/or wire activity, is determined to be high.

**Money Laundering Risk Ratings for New Online Accounts**

[Insert Financial Institution Here] recognizes that accounts which are opened without face-to-face or phone contact may pose a higher risk for money laundering for the following reasons:

* More difficult to positively verify the individual’s identity;
* Customer may be out of [Insert Financial Institution Here]’s targeted geographic area;
* Customer may perceive the transactions as less transparent;
* Transactions are instantaneous; and/or
* May be used by a “front” company or unknown third party.

The Bank will obtain the same information as it would for a face-to-face account opening and will use ChexSystems’ QualiFile electronic inquiry response to authenticate identity.  The Bank has limited the geographic availability to New York, New Jersey, and Connecticut.  Due to the above considerations, all new online accounts will be deemed medium risk for the first three (3) months and if there is no unusual activity for that time period, then the account will be changed to low risk.  Pursuant to the Bank’s two (2) year periodic review process for medium risk accounts, if the customer’s activity warrants a change in risk rating, then the Bank will act accordingly.

Please refer to the Bank’s Account Create Procedures.

Additional KYC Due Diligence Requirements for Certain Customers, Related Parties, and Accounts

**New High-Risk Customers**

All new customer relationships that are deemed high-risk, and those escalated from medium or low to high-risk, are subject to review by the AML Officer. The Standard Account Review Sheet is subject to completion, and review based on established requirements. If, upon review, the AML officer deems that the Bank cannot continue with this relationship, the AML officer will make a recommendation to close the account. Any decision to keep the account open after such recommendation will require approval from the Chairman of the Board.

***Refer to Appendix G for Standard Account Review Sheet***

**Politically Exposed Persons**

Customers/related parties who are Politically Exposed Persons (PEPs) increase the risk that the Bank could be exposed to involvement in money laundering or other illegal activities. The financial activities of PEPs may be of public interest or might otherwise attract publicity within or beyond the borders of their home country, and their transactions with the Bank could potentially involve the proceeds of foreign official corruption. If the Bank knowingly engages in financial transactions in violation of the money laundering laws of various jurisdictions, the Company will be exposed to significant legal and reputational harm.

PEPs are defined as a U.S. or non-U.S., current or former, senior official of the executive, legislative, administrative, military or judicial branches of a government, whether elected or not and include senior officials of a major political party or a senior executive of a government-owned commercial enterprise. A senior official or executive is defined as an individual with substantial authority over policy, operations, or the use of government owned services. PEP positions include, but are not limited to:

* Heads of State, Government Heads or National Leaders, such as the President, Prime Minister, King, Queen, Emir, Sultan, Emperor, Monarch, Pope
* National Cabinet Members and Department/Agency Heads, such as the Vice President, Chancellor, Secretary of State, Defense Minister, Chief of the Treasury, Head of the National Bank, and other key Department, Agency, Ministry, and Office Officials
* Key National Legislative Officials, such as Congressmen, Senators, House Representatives, Parliament members, Assemblymen, Councilmen
* Senior Military Leaders, such as the Army Secretary
* Important National Justices, such as the Attorney General, Chief Justices, and Associate Judges
* Political Party Leaders
* Ambassadors/Consuls General, including the United Nation Representative
* Governors
* Mayors of cities with populations in excess of 1MM
* Senior executives of government-owned enterprises, such as the Chairman, CEO and President of government airline.

The following customers/related parties are also PEPs and are therefore bound by the requirements of this section:

* Corporations, businesses or entities formed by, or for the benefit of, or significantly owned or controlled by, a PEP; significant ownership is 25% or more; control includes holding a senior executive position of influence, such as the Chairman, CEO, and President
* Any immediate family member of a PEP, including the spouse, parents, siblings, children, and spouses’ parents or siblings
* A person who is widely and publicly known to be a close associate of any such individual
* Foreign Embassies/Consulates/Ministries
* Foreign political organizations.

Upon account opening, reasonable steps will be taken to determine whether customers and related parties are PEPs including the direct inquiry with the customer. The customer’s KYC profile and account record must indicate that the client is a PEP.

Enhanced scrutiny is required whenever the Bank does business with a PEP. This enhanced scrutiny includes the following:

* Determining the identity of the PEP
* Assessing the level of corruption and characteristics associated with the PEP’s country
* Evaluating the PEP’s position, length of time in office, and reputation
* Probing the PEP’s employment history and source of funds and wealth
* Obtaining information on immediate family members or close associates having transaction authority over the account
* Understanding the purpose of the account and expected volumes and nature of account activity
* Considering the use of the account(s)
* Performing appropriate database/internet checks to gather information
* Obtaining Board of Directors approval before account opening (presentation to outline the nature of the request, explanation of the rationale for initiating or maintaining the PEP relationship and providing adequate information regarding the PEP, the due diligence steps taken in regard to the relationship and how the PEP’s ongoing activities with Bank will be monitored.)
* On an annual basis, each Business Head must review the PEPs in his or her business to determine if their retention continues to be appropriate. This review must be evidenced in writing.

***Refer to “PEP Scanning Procedures” for detailed processes for identifying Politically Exposed Persons.***

**Money Services Businesses**

Money Service Businesses (MSBs) are high-risk because many:

* Lack ongoing customer relationships and require minimal or no identification of customers
* Maintain limited or inconsistent recordkeeping on customers and transactions
* Engage in frequent currency transactions
* Are subject to varying levels of regulatory requirements and oversight
* Can quickly change their product mix or location and quickly enter or exit an operation
* Sometimes operate with improper registration or licensing

MSBs are defined as any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

* Currency dealer or exchanger
* Check casher, including “payday” loan and check cashing services
* Issuer of traveler’s checks, money orders or stored value products
* Seller or redeemer of traveler’s checks, money orders or stored value products (including the United States Postal Service)
* Money transmitter

It is the policy of the Bank not to do business with MSBs, except for:

* U.S. or state-regulated mortgage banking firms
* Recognized national or regional retail chain stores whose principal business is not money services.

For any other MSBs, Board of Directors approval is required. In addition, the following baseline due diligence must be performed for all MSB relationships:

* Confirm that the MSB is registered with FinCEN
* Confirm state and local licensing, if applicable
* Confirm agent status, if applicable
* Conduct an on-site visit
* Determine and review the ownership or senior management of the MSB.
* Conducting a risk assessment of the MSB
* Confirmation of MSB’s understanding that it will be subject to federal and state bank regulatory oversight in connection with activities conducted with and through CRB
* Determining whether necessary insurance coverage, continuity plans, policies and procedures are in place
* Identifying the MSB’s customers’ profile, potential issues, risks and concerns, and areas of customer complaints
  + Determining whether any conflicts of interest exist between management and insiders of CRB;
  + Developing an MSB questionnaire to obtain additional information about each customer’s business. The questionnaire will ask the customer for information on its products and services, customer base, types of software used, employee training procedures, and other information; and
  + Requesting copies of the MSB’s BSA/AML and OFAC policies and procedures.
  + IT due diligence (depending on customer’s business model)

As part of its ongoing due diligence, the Bank will conduct periodic site visits of MSB customers. In addition, MSB customers are required to periodically furnish the bank with: updated, board approved policies and procedures; and independent review of the BSA/AML program and management response.

***Refer to the “MSB White Paper” for details regarding MSB due diligence.***

**Hedge Funds**

Hedge funds may be higher-risk because they provide customers with offshore investment vehicles. Hedge funds are similar to mutual funds in that they both are pooled investment vehicles that accept investors’ money and generally invest it on a collective basis. Hedge funds differ significantly from mutual funds, however, because hedge funds are not regulated.

Before opening an account for a hedge fund, the following due diligence will be performed:

* Obtain and review a prospectus, offering document or other documentation describing the fund
* Record the name of and background information for the investment advisor/management company and/or the general partners or other similar senior officers, such as the Chief Executive Officer, Chief Administrative Officer, Chief Information Officer, etc.
* Perform OFAC screenings on the fund, the investment advisor/management company, and/or the general partners or other similar senior officers by conducting Internet research or another similar service or third-party confirmation.

**Onboarding of Peer-to-Peer Lending Companies**

[Insert Financial Institution Here] will partner with one or several Peer-To-Peer Lending Companies (“P2P”) to issue unsecured consumer and business loans to borrowers with certain credit profiles. The Bank requires each P2P lending company to develop and implement a written BSA/AML program that is reasonably designed to prevent the company from being used to facilitate money laundering or the financing of terrorist activities. At a minimum, the anti-money laundering program shall: provide for policies and procedures to prevent money laundering and detect suspicious activity; designate a compliance officer; provide for ongoing training of appropriate persons; and provide for periodic independent testing of the AML program. The Bank also requires each P2P lending company to adopt a Customer Identification Program that is in compliance with the Bank’s Customer Identification policies.

The selection of the P2P lending companies will be based on, but not limited to, the following:

* Adequacy of BSA/AML policies and procedures
* Review of results from compliance, BSA/AML and IT audits

Bank management will request that BSA/AML audits be performed prior to the commencement of any funding. For new companies, a 2-step process will be employed whereby the policies will be reviewed for adequacy and control and the transaction testing will be performed 60 days after program launch. The results will be reviewed thoroughly, and findings will be detailed in a memo to the BOD.

***Refer to the “Peer-to-Peer Lending Policy” for a detailed description of the requirements for P2P lending companies***

**Reliance on Others**

In those instances in which a financial intermediary introduces its client to the Company and the intermediary’s customer opens an account and/or otherwise enters into a contractual relationship with one or more of the Bank’s business units, KYC due diligence on the contracting party is the responsibility of the business unit; however, businesses are permitted to rely on the customer identification and verification procedures of another financial institution to establish the identity of the customer. Reliance, for purposes of such safe harbor, is appropriate when the other financial institution has established a similar banking/business relationship with the customer to that of the Company and when such reliance can be considered reasonable under the circumstances. In order to be able to rely on the customer identification procedures of another financial institution, the other entity:

* Must be subject to the AML program requirements set forth in the USA PATRIOT Act and implementing regulations
* Must be regulated by a U.S. Federal functional regulator, and
* Must enter into a contract with the Bank requiring the other financial institution to certify annually that it has implemented its AML program and that it, or its agent, will perform the customer identification and verification program requirements.

In instances in which the intermediary to be relied upon is not subject to the requirements of the USA PATRIOT Act, that intermediary:

* Must be subject to money laundering control requirements under its local laws and regulations
* Must be regulated by a recognizable financial services regulator in the country of jurisdiction
* Must provide a letter of attestation to the Bank in which its attests to its compliance with all appropriate customer identification, verification, and other due diligence requirements.

In all cases in which a business is placing reliance upon an intermediary for the performance of any customer identification or other KYC due diligence steps, the prior, written approval must be obtained from the BSA/AML Compliance Officer. This approval is required whether the entity relied upon is U.S. or non-U.S. intermediary.

*KYC information provided by new employees who bring customers with them from other financial institutions must be independently obtained and verified by someone other than the new employee.*

**Ongoing Relationship/Customer/Account Activities**

KYC records are intended to be dynamic and enhanced over time as knowledge of a customer grows. The relationship owner will review and update KYC information whenever significant changes in activity, ownership, or public information about the client become known.

The Bank uses an automated monitoring system in order to monitor account activity, on an on-going basis. The automated monitoring system analyzes transactions for unusual activity, and generates alerts for review. A Compliance Analyst reviews these alerts on a daily basis.

Also in regard to the ACH environment, the Operations Department will review the following reports on a daily basis for unusual activity and scanning:

* Entries – Checking PL6570-01
* Entries – Savings PL6570-06
* Originating Entries PL5500-02
* OFAC Screening – Org Final PL6579-04 (IATs)
* OFAC Screening – Receiving Final PL6579-02 (IATs)
* OFAC Screening – ACH OFAC Rec (PL6579-01)
* ACH Originating Activity (PL2000-02)
* Return/NOC Activity Listing (PL2000-01)
* Special Edits Updates (PL6564-01)
* Death Notification Report
* International (IAT) RDFI Report
* Receiver Setup Report
* Notification of Change ODFI Report
* Originator Setup Report
* Return Item-ODFI Report

In addition to the daily reports, the following ACH reports are reviewed monthly

* ACH Volume Report per Originator
* Return Ratio Report per Originator

Unusual activity may encompass the following:

* Reviewing originators/recipients’ whose business or occupation does not warrant the volume or nature of ACH activity;
* Originators whose origination activity suddenly exceeds projections/credit-debit limits with no reasonable explanation for such change;
* Originators generating a high rate or high volume of invalid account returns or a high-rate or high volume of unauthorized returns/transactions;
* Specific returns creations (RDFI) covering unauthorized, fraudulent, or revoked transactions, and Federal reclamations.

Unusual conditions will be investigated and handled appropriately by the reviewer. Such examination of these daily reports must be evidenced by the reviewer by initialing the Daily Account Review Log or the report printout.

In order to monitor ongoing wire transfer records quarterly, the branch manager/designee will review the Wire Transfer Velocity Report for questionable and/or unusual patterns. Particular attention will be paid to incidents where:

* Unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity;
* A large number of wire transfers to or from unrelated third parties inconsistent with the customer’s legitimated business purpose;
* Wire transfers that have no apparent business purpose to or from a foreign country;
* The customer’s account has inflows of funds or other assets well beyond the known income or resources of the customer;
* Transactions in which the primary beneficiary or counter-party is undisclosed.   
    
  The branch manager/designee will sign the quarterly report as evidence that the quarterly review was conducted.

*Unusual Activity Detected by a P2P Lending Company:* Each Peer-To-Peer Lending Company (P2P) that [Insert Financial Institution Here] (the Bank) partners with is required to have an Anti-money Laundering program. As part of the program, the P2P lending company must have policies and procedures to detect and identify suspicious activity. When a P2P lending company identifies suspicious activity, they notify the Loan Service Department at [Insert Financial Institution Here] of the unusual activity. The Loan Service Department works with the P2P lending company to prepare an Incident Report. A Compliance Analyst and the Bank’s AML/BSA Officer, review the incident report to determine whether the activity warrants a Suspicious Activity Report filing.

*Suspicious Activity Report (SAR) Filing:* Upon detection of unusual activity, it is the Bank’s policy to file a SAR with respect to:

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

*Note: Because elderly individuals experience declining cognitive or physical abilities, they are more reliant on specific individuals for their physical well-being, financial management, and social interaction. Therefore, certain elderly individuals may be particularly vulnerable to identity theft, embezzlement, and fraudulent schemes. See Appendix I for Possible Signs of Elder Financial Exploitation.*

An investigation will be conducted for any activity deemed suspicious and if necessary, a SAR will be filed.

This Policy provides for a process of periodic, risk-based customer relationship reviews. In the absence of an event that calls immediate attention to a relationship or to activity in the customer’s accounts, the periodic review provides the Bank with the opportunity to update KYC information, review the customer’s recent transactions and interactions with the Bank, and reaffirm that retaining the relationship continues to be appropriate.

The periodic review is to be performed by the relationship owner and should:

* Ensure that KYC information is accurate, complete, and up-to-date
* Consider the effects of any significant inflows, outflows, and any obvious changes in the accounts’ purposes, for appropriateness and consistency with expectations.
* Evaluate the customers’ general transaction volumes and overall balances across all products and services for reasonableness and consistency with the customer’s financial situation and the relationship’s stated purpose.

Periodic reviews will occur at least every 12 months for high-risk customers and 24 for medium-risk customers. The first month of each quarter, high risk accounts having a yearly anniversary in that quarter, based on the date of the assigned risk rating, will be identified. During that three-month period, a review will be performed using the Standard Account Review Sheet. The review method for medium risk accounts would be the same but based upon a two-year anniversary of the assigned risk rating date. The Standard Account Review Sheet is subject to the necessary review and approval based on established requirements.

***Refer to Appendix G for Standard Account Review Sheet***

**Special Measures**

The USA PATRIOT Act gives the Secretary of the Treasury authority to impose special measures against foreign jurisdictions, foreign financial institutions, transactions involving such jurisdictions or institutions, or one or more types of accounts, that are determined to pose a “primary money laundering concern” to the United States.

The BSA/AML Compliance Officer will coordinate compliance with such special measures on a bank-wide basis. It is the policy of the Bank to promptly comply with any special measures prescribed by the Secretary of the Treasury. Whenever the Secretary imposes special measures, Compliance shall communicate the special measures to the affected businesses, which will take the steps necessary to terminate affected account relationships, communicate to customers, and/or amend existing policies, procedures, and controls or develop new ones to comply with the prescribed special measures.

**Information Sharing**

The USA PATRIOT Act provides for information sharing between the Government and Financial Institutions, as well as between financial institutions themselves, in an effort to deter money laundering and terrorist activities.

Section 314(a) of the Act establishes a mechanism for law enforcement agencies to communicate the names of suspected terrorists and money launderers to covered financial institutions for the purpose of promptly identifying accounts and transactions involving those suspects. Under 314(a), information requests are batched and forwarded to covered financial institutions from FinCEN every two weeks (although single requests may be sent in urgent situations). *Note: The designated points of contact for receiving 314(a) are reflected on the Bank’s Call Report Filings.*

Upon receipt of a 314(a) request, Company covered financial institutions are required to search the following records:

* Deposit account records
* Funds transfer records
* Records for the sale of monetary instruments
* Loan records

The Bank will search its records for the preceding 12 months for accounts, and for the preceding 6 months for transactions, and report them to FinCEN. As the Bank has several third party, and marketplace lenders, in addition to the scan of accounts, and transactions, the Bank will conduct a FinCEN scan for any retained loans as well as any loans funded within the last 12 months. If other matching records are found in this process, they will also be reported to FinCEN, even if they fall outside of the requested time frame or pertain to an account or transaction in an area of the financial institution that was not required to be searched but were searched anyway, or pertain to a record that was not required to be maintained under federal law or regulation but existed nonetheless.

Searches are required to be completed and a response to be sent to FinCEN with any matches within two weeks of receiving the 314(a) request.

If there is a positive match for an account or a transaction, the following information will be gathered:

* The identity of the individual, entity, or organization
* The account number(s); opening date, type of transactions
* All identifying information provided by the account holder in connection with the opening of the account, such as social security number, taxpayer identification number, passport information, date of birth, and address.

Names are highly confidential and should be shared only on a limited basis. Under no circumstances should 314(a) names be shared with any other financial institution. Records regarding 314(a) searches must be retained in a secure area.

If the 314(a) search results in a positive match, it is incumbent upon the Bank to conduct an investigation of the account relationship and/or transaction activity and should there be reasonable belief that suspicious activity occurred, an Incident Report must be drafted for SAR consideration.

If the Bank decides to close the account, it will first notify the law enforcement contact on the request to determine if closing the account would interfere with an active investigation. If law enforcement requests that an account remain open, the bank will request written confirmation.

Note: The bank does not participate in 314(b)

***Refer to Appendix H for procedures concerning responses to information requests***

**Subpoenas Received from Law Enforcement**

The receipt of a grand jury subpoena will cause the bank to conduct a risk assessment and account relationship review of the subject customer. The information resulting from the review, transactions, and accounts subject to the subpoena will be evaluated and a determination will be made as to whether additional account monitoring should be implemented, or a suspicious activity report filed.

**Currency Transaction Reporting and Exemptions**

In compliance with the BSA regulations, the following types of reports are submitted to the U.S. government:

* FinCEN Form 112, Currency Transaction Report (CTR): A CTR must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of more than $10,000. Multiple currency transactions must be treated as a single transaction if the financial institution has knowledge that: (a) they are conducted by or on behalf of the same person; and, (b) they result in cash received or disbursed by the financial institution of more than $10,000. A CTR must be filed within 15 days electronically from the date of the transaction with FinCEN. The bank must retain copies of CTRs for five years from the date of the report.
* FinCEN Form 105, Report of International Transportation of Currency or Monetary Instruments (CMIR): Each person who physically transports, mails or ships, or causes to be physically transported, mailed, shipped or received, currency, traveler’s checks, and certain other monetary instruments in an aggregate amount exceeding $10,000 into or out of the United States must file a CMIR.

The preparation process of these reports will be through the Bank’s automated monitoring system. The automated monitoring system loads Cleartouch data into the system, and when reportable transactions are found, auto-generates populated CTRs. The branch manager is responsible for performing a secondary review to ensure accuracy and submitting the report.

Currency transactions over $3,000 are recorded daily on the “Currency Transactions Greater Than $3,000 Log”. Daily, this log is reviewed by the branch manager/designee to ensure that multiple currency transactions totaling over $10,000 for a customer are properly reported. This log also must be reviewed for possible structuring situations and initialed as evidence of review. On a monthly basis, the branch manager/designee will review this report on a cumulative basis to detect patterns or structuring trends. The branch manager/designee will evidence this review by signing this monthly report.

Structuring is the breaking up of transactions for the purpose of evading the BSA reporting and recordkeeping requirements and, if appropriate thresholds are met, should be reported as a suspicious transaction. Structuring may be indicative of underlying illegal activity; further, structuring itself is unlawful under the BSA.

Penalties and asset forfeiture for money laundering can be severe under BSA:

* Individuals, including employees of financial institutions, convicted of money laundering face up to 20 years in prison for each money-laundering transaction.
* Businesses, including banks and individuals, face fines up to $1,000,000 or twice the value of the transaction, whichever is greater.
* Financial Institutions can lose their charter/license, and employees risk being removed and barred from the business.
* Any property involved in the transaction or traceable to the proceeds of the criminal activity, including loan collateral, personal property and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate) may be subject to forfeiture.

**Safe Harbor Provision**

The Annunzio Wylie Anti-Money Laundering Act (1992) – U.S.C. 5318(g)(3) - provides a safe harbor for the bank and its employee from civil liability for reporting known or suspected criminal offenses or suspicious activity by filing a SAR. A bank employee should feel safe in reporting suspicious activity. The government works closely with the bank to ensure that all employees are protected from any liability.

**Federal Law prohibits Employees from disclosing the fact that a SAR has been filed. Never discuss any Suspicious Activity Reporting requirements with a customer. Voluntarily giving additional information to customers, such as when you completed an incident report for their suspicious activity makes the employee liable for prosecution for violating Anti-Money Laundering Laws.**

**Recordkeeping and Record Retention Requirements**

The following rules apply to CIP-related records:

* Identifying information (name, address, date of birth, and government-issued ID number) must be retained for five years after the date the account is closed
* All other information and documentation required by CIP rules, such as other recorded customer information, copies of documents used to verify identity, records of the steps taken and the results of verification performed by non-documentary means, and the resolution of discrepancies that may have arisen between information provided by a customer and the documentary and non-documentary evidence used to verify such information, must be retained for five years after the record is made.

KYC-related records can be maintained in either hard copy or in electronic form, so long as the records are accurate and readily accessible within five calendar days.

The Bank must maintain a record of each funds transfer of $3,000 or more, which it originates, acts as an intermediary for, or receives for five years. The amount and type of information that must be recorded and kept depends upon the Bank’s role in the funds transfer process. Also, the Bank must pass certain information along to the next bank in the funds transfer chain when it acts as an originator or intermediary for a funds transfer

|  |  |
| --- | --- |
| **Transmitter’s Financial Institution** | **Intermediary Financial Institution** |
| Name and account number of the transmitter | All of the information included in the payment order by the transmitter’s financial institution, plus; |
| Address of the transmitter | Name and address or numerical identifier of the transmitter’s financial institution |
| Identity of the transmitter’s financial institution |  |
| Amount of the transmittal |  |
| Execution date of the transmittal order |  |
| Identity of the recipients’ financial institution |  |
| And as many of the following items as are received with the transmittal: |  |
| Name and address of the recipient |  |
| Account number of the recipient |  |
| Other specific identifiers of the recipient |  |

The Bank which provides for the purchase and sale of monetary instruments must require the retention of records of cash sale to a customer for bank checks, drafts, cashier’s checks, money orders, and traveler’s checks (which the Bank does not currently sell) between $3,000 and $10,000 inclusive for five years. These records must include evidence of verification of the identity of the purchaser and other information as outlined below:

* The name of the purchaser;
* Date of purchase;
* Types of instrument purchased;
* Serial number of the instrument purchased;
* The amounts in dollars of each of the instruments purchased; and
* Verification that the individual is a deposit holder/verification or the purchaser’s identity (address, SS#/Alien Identification #, DOB).

*The following records will be retained for seven years:*

* *A record of each extension of credit in an amount in excess of $10,000*
* *Each document granting signature authority over each deposit or share account*
* *Each statement, ledger card or other record on each deposit or share account, showing each transaction in, or with respect to, that account*
* *Each check, clean draft, or money order drawn on the Company or issued and payable by it*
* *Each item in excess of $100 comprising a debit to a customer’s deposit or share account*
* *Records prepared or received in the ordinary course of business, which would be needed to reconstruct a transaction account and to trace a check in excess of $100*
* *Each deposit slip or credit ticket reflecting a transaction in excess of $100.*

**AML Training**

Annually the Bank shall maintain a regular training program for the purpose of educating its personnel and heightening their awareness so that they will be knowledgeable and vigilant in their efforts to recognize and report activity, which may constitute money laundering.

Within 60 days of hire, new employees will be trained in the basic aspect of AML. Additionally, the new employee will be required to read and attest that they understand the contents of the Bank’s AML/BSA policies.

The appropriate attendance records and training materials will be retained for three years.

*Note: Training will be conducted at least annually for the Board of Directors.*

**BSA/AML Compliance Officer**

The BSA/AML Compliance Officer has day-to-day responsibility for managing all aspects of the Bank’s AML Program and compliance with AML laws and regulations. The BSA/AML Compliance Officer is also responsible for the maintenance of this Policy and for considering deviations to this Policy. In addition, the BSA/AML Compliance Officer advises staff regarding the application of anti-money laundering laws and regulations and on money laundering trends and patterns specific to certain businesses.

Despite changes in management or employee composition or structure, the BSA/AML Compliance Officer will ensure that all requirements of an effective BSA/AML program are implemented and that the program contains all appropriate aspects to be in compliance with all laws and regulations.

**BSA/AML Risk Assessment**

The Bank has developed a risk assessment, which was approved by the Board of Directors, by identifying risks along with the associated mitigants. The assessment will be periodically reviewed and presented to the Board for approval.

**Independent Testing**

Independent testing commensurate with the BSA/AML risk profile of the bank will be conducted every 12 to 18 months by outside auditors. Upon completion, the auditors conducting the BSA/AML test will report the results to the Audit Committee.

**Board Reporting**

On an annual basis or more frequently as circumstances dictate, the BSA/AML Compliance Officer will present a report to the Board of Directors. This report will include such important facts relating compliance initiatives, any deficiencies/corrective action noted, SAR filings relating to AML, etc.

# **APPENDIX A**

**EXAMPLES OF SUSPICIOUS CONDUCT AND TRANSACTIONS**

The existence of one or more of these suspicious circumstances does not mean that money laundering activity is taking place, but that such circumstances should be scrutinized carefully.

* Customers who are reluctant to provide normal information when opening an account or who provide fictitious or conflicting information.
* Customers with no discernible reason for using the Bank’s services (e.g. customers with distant addresses who could find the same services nearer to home)
* Business customers who are reluctant to provide complete information regarding the purpose, prior banking relationships, officers or directors, or location of their business.
* Business customers who are reluctant to reveal details about their activities, or to provide financial statements, or whose financial statements are noticeably different from those of similar businesses.
* Large cash deposits by an individual or business where checks and other instruments are the expected norm.
* Structuring multiple cash deposits which are individually unexceptional, but significant in the aggregate.
* Exchanging large quantities of low denomination currencies for those of higher denomination.
* Deposit or withdrawal activity that is inconsistent with the activity normally associated with the customer or the customer’s type of business.
* Funds transfers are sent or received from the same person to or from different accounts.
* Funds activity is unexplained, repetitive, or shows unusual patterns.
* A customer uses unusual or suspicious identification documents that cannot be readily verified.
* The customer’s background differs from that which would be expected on the basis of his or her business activities.
* A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
* A person uses the automated teller machine to make several bank deposits below a specified threshold.
* The currency transaction activity reflected a sudden change inconsistent with normal activities.
* A customer purchases a number of cashier’s checks, money orders, or traveler’s checks for large amounts under a specified threshold.
* Suspicious movements of funds occur from one bank to another and then funds are moved back to the first bank.
* Deposits of large third-party checks endorsed in favor of the customer where such conduct is inconsistent with the customer’s normal activity.
* Large numbers of individuals making payments into the same account without adequate explanation.
* Unexpected repayment of problem loans.
* Requests to provide or arrange financing where the source of the customer’s financial contribution to a deal is unclear, particularly where property is involved.
* Employees whose habits or lifestyles change unexpectedly
* Employees whose performance changes unexpectedly.
* The stated occupation of the customer is not commensurate with the type of level of activity.
* Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

***For additional examples of Money Laundering and Terrorist Financing “Red Flags” see the FFIEC BSA/AML Examination Manual 11/17/2014.***

# **APPENDIX B**

**COUNTRY TIERING LIST**

**Tier 1**

**Afghanistan Albania Angola**

**Anguilla Antigua/Barbuda Argentina Armenia**

**Azerbaijan Bahamas Bangladesh Belarus**

**Belize Bolivia Botswana Brunei**

**Burkina Faso Burundi Cambodia Cameroon**

**Cape Verde Chad Colombia Congo**

**Costa Rica Cuba Cyprus Dominican Republic**

**East Timor Equatorial Guinea Eritrea**

**Estonia Ethiopia Gabon Gambia**

**Georgia Ghana Grenada Guinea**

**Guinea-Bissau Haiti Honduras Indonesia**

**Iran Iraq Ivory Coast Kazakhstan**

**Kenya Kuwait Kyrgyzstan Laos**

**Latvia Lebanon Lesotho Liberia**

**Libya Lithuania Macau Malawi**

**Maldives Mali Mexico Moldova**

**Mongolia Montenegro Montserrat Morocco**

**Myanmar Namibia Nauru Nepal**

**Nicaragua Nigeria Niue North Korea**

**Pakistan Palestinian Panama Papua New Guinea**

**Paraguay Peru Philippines Russia**

**Rwanda Sao Tome&Principe Serbia/Montenegro Seychelles**

**Sierra Leone Soloman Islands Sri Lanka St. Lucia**

**Syria Tajikistan Tanzania**

**Thailand Trindad & Tobago Turkey Turkmenistan**

**Uganda Ukraine Uzbekistan Venezuela**

**Vietnam Yemen Zambia Zimbabwe**

**Tier 2**

**Akrotiri Sovereign Aland Islands American Samoa Andorra**

**Antarctica Aruba Ashmore & Cartier Azores**

**Baker Island Benin Bermuda Bhutan**

**Bouvet Island Brit Virgin Islands British Oceania Canary Islands**

**Cayman Islands Central African Re Christmas Island Clipperton Island**

**Cocos Comoros Congo Cook Islands**

**Coral Sea Islands Croatia Dhekelia Sov Base El Salvador**

**Falkland Islands Faroe Islands Fed St Micronesia Guiana**

**French Polynesia French Southern Ghana Gibraltar**

**Greece Greenland Guadeloupe Guam**

**Guatemala Guernsey Guyana Heard/Mcdonald Is**

**Howland Islands India Indonesia Isle of Man**

**Jamaica Jarvis Island Jersey Johnston Atoll**

**Jordan Kingman Reef Kiribati Kosovo**

**Liechtenstein Macedonia Madagascar Madiera**

**Malaysia Marshall Islands Martinique Mauritania**

**Mayotte Midway Islands Monaco Mozambique**

**Navassa Island Neth Antilles New Caledonia Niger**

**Norfolk Island North Mariana Is Palau Palmyra Atoll**

**Paracel Islands Pitcairn Islands Qatar Reunion**

**Saint Helena San Marino Saudi Arabia Senegal**

**Somalia South Georgia South Korea South Sandwich Islands**

**Spratly Islands St Barthelemy St Pierre/Miquelon St Kitts/Nevis**

**St. Martin St Vincent & Gren Suriname Svalbard/JanMayen**

**Togo Tokelau Tonga Turks/Caicos**

**Tuvalu US Virgin Islands United Arab Emirates**

**Uruguay Vanuatu Vatican City Wake Island**

**Wallis & Futuna Western Sahara Western Samoa**

**Tier 3**

**Bahrain Barbados Bosnia-Hercegovina Bulgaria**

**China Djibouti Dominica Egypt**

**Fiji Hong Kong Hungary Israel**

**Luxembourg Malta Mauritius Oman**

**Poland Puerto Rico Romania Singapore**

**Slovakia Slovenia South Africa Swaziland**

**Switzerland Taiwan Tunisia**

**Tier 4**

**Australia Austria Belgium Brazil**

**Canada Chile Czech Republic Denmark**

**Finland France Germany Iceland**

**Ireland Italy Japan Netherlands**

**New Zealand Norway Portugal Spain**

**Sweden United Kingdom United States**

|  |  |
| --- | --- |
| **Primary**   * Driver’s License (US or Canada) * Military ID with Photo (US) * Passport with Photo (US) * US Federal or State Government Employee ID with Photo * Senior/Disabled Only – If a senior (age 55 and older) or disabled person is unable to provide one of the above forms of primary ID, the and only then are following ID acceptable:   **-Human Services ID with Photo- Federal, state or local government US issued only.**   * Minors Only – If a minor (under 18) is unable to provide of the above primary forms of ID then the following forms of ID are acceptable:   - **Birth Certificate(US)**  **-Social Security Card** | **Secondary**   * Any form of Primary ID for US Citizens * Bank Statement- dated within the last 60 days and includes name and street address(includes deposit, loan, credit card, brokerage and investment accounts) * Major Credit Card with Signature and Embossed/Imprinted Name(excludes gift cards, store valued cards, and Department store cards) * Other US Federal/State- issued ID(for example Learner’s Permit) * Student ID with Photo * Student Letter – A letter from a school with a current date or not more than one year old which includes the customer’s name/university * Utility Bill – dated within 60 days and includes name and street address(includes cable home/cell phone, electric, or gas) * Senior/Disabled Only – If a senior (age 55 and older) or disabled person is unable to provide one of the above forms of primary ID, the and only then are following ID acceptable:   **-Medicare/Medicaid Card (US)**  **-Organization Membership (US) (ie AARP, United Workers Union, etc)**  **-Other Insurance Card**  **-Social Security Card**  **-Voter Registration Card (US**)   * Minors Only – If a minor (under 18) is unable to provide of the above primary forms of ID then the following forms of ID are acceptable:   - **Birth Certificate(US)**  **-Social Security Card** |

# **APPENDIX C**

**DOCUMENTARY VERIFICATION DOCUMENTS – US Citizens**

|  |  |
| --- | --- |
| **Non US Citizens** | |
| **If non Resident Alien has a US address, one piece of ID must be foreign-issued to support foreign status.** | |
| Primary ID | Secondary ID |
| **One** of the following Primary IDs:   * Canadian Driver’s License with Photo * US Drivers License with Photo (can only be used by Resident Aliens with SSN or ITIN * Employment Authorization Card with Photo (issuer: US Department of Homeland Security or US Department of Justice) * Passport with Photo (Foreign) * Permanent Resident Card with Photo (Can only be used by Resident Aliens) | **One** of the following SECONDARY IDs:   * Any form of acceptable Primary not already used * Foreign National Id (includes foreign government issued driver’s license, vehicle operator’s license) * Major Credit Card w/Signature & Embossed/Imprinted Name * Student ID with Photo * Student Letter – A letter from a school with a current date or not more than one year old which includes the customer’s name/university * Temporary Resident Card with Photo * Utility Bill – dated within 60 days and includes name and street address (includes cable home/cell phone, electric, or gas) * United Nations Letter- A letter from the UN, Consulate, Embassy, or UN Mission which includes customer’s name, employer’s name, and U.S. & Non-U.S. residential address. |
| Additional Acceptable Primary IDs for Resident Aliens who can provide SSN/ITIN | Additional Acceptable Secondary IDs for Resident Aliens who can provide SSN/ITIN |
| * Military ID with Photo * State Identification Card with Photo(US) * US Federal or State Government Employee ID * Social Security Card (US)-Minors (under 18 only) | * Human Services ID (US) (ie welfare assistance card) * Medicare/Medicaid Card – (US) Seniors (Age 55 and older) and/or Disabled only * Social Security Card (US) Seniors (age 55 and older) and/or Disabled and Minors (under 18 only) |

Required Business Documentation

|  |  |  |
| --- | --- | --- |
| **Legal Entity** | **Documents Provided by Customer** | **[Insert Financial Institution Here]** **Forms Required** |
| Corporation | Filed copy of Certificate of Incorporation  **OR**  Filing Receipt with the State Seal  **OR**  Certificate of Good Standing  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) –  If entity formed outside the State of New Jersey has a physical business location in the state of New Jersey, then a Certificate of Authority issued by the State of New Jersey **must** be provided. | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card |
| Limited Liability Company (LLC) | Certified copy of Articles of Organization  **OR**  Certified copy of Certificate of Formation  **OR**  Filing Receipt with the State Seal  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) –  If entity formed outside the State of New Jersey has a physical business location in the state of New Jersey, then a Certificate of Authority issued by the State of New Jersey **must** be provided. | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card |
| General Partnership | Certified Copy of Partnership Certificate  **OR**  Certified Copy of Business Certificate  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) -  If entity formed outside the State of New Jersey has a physical business location in the state of New Jersey, then a Certificate of Authority issued by the State of New Jersey **must** be provided. | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card |

|  |  |  |  |
| --- | --- | --- | --- |
| **Legal Entity** | | **Documents Provided by Customer** | **[Insert Financial Institution Here]** **Forms Required** |
| Limit Liability Partnership(LLP) | Certified Copy of Registration  **OR**  Certified copy of General Business Certificate  **OR**  Certified copy of Partnership Agreement  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) –  If entity formed outside of the State of New Jersey or New York has a physical business location in the state of New Jersey then a Certificate of Authority issued by the State of New Jersey **must** be provided. | | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card | |
| Limited Liability Limited Partnership (LLLP) | Certified Copy of Registration  **OR**  Certified copy of General Business Certificate  **OR**  Certified copy of Partnership Agreement  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) –    If entity formed outside the State of New Jersey has a physical business location in the state of New Jersey then a Certificate of Authority issued by the State of New Jersey **must** be provided. | | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card | |
| Sole Proprietorship | Trade Name Certificate  **OR**  Business Name Certificate  **OR**  Business License  Note: Professionals do not require an Assumed Name Certificate i.e. Physicians, Attorneys, CPAs) | | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card | |
| Joint Venture | Assumed Name Certificate with filing stamp (if applicable)  **AND**  Joint Venture Agreement  **OR**  External Business Resolution  **AND**  TIN provided by the entity | | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Legal Entity** | | **Documents Provided by Customer** | **[Insert Financial Institution Here]**  **Forms Required** | | |
| Unincorporated Business Association/Organization | Certificate of Good Standing  **OR**  Articles of Association  **OR**  Charter Document validating existence of association/organization  **AND**  TIN provided by the entity  **AND**  Certificate of Authority (where applicable see below) –  If entity formed outside the State of New Jersey has a physical business location in the state of New Jersey then a Certificate of Authority issued by the State of New Jersey **must** be provided. | Business Depository Resolution  [Insert Financial Institution Here]  Signature Card | |
| Public Funds | Incumbency Document  **OR**  External Business Resolution  **OR**  Letter or Meeting Minutes granting authority | [Insert Financial Institution Here]  Signature Card | |
| Estate | Certificate of Issuance of Letters of Administration  **OR**  Certificate of Issuance of Letters of Testamentary  **OR**  Surrogates Certificate | [Insert Financial Institution Here]  Signature Card |
| Trust | Copy of the first page and the page that designates the trustees; generally, the last page. The notary section must be included.  **AND**  TIN provided by the entity | [Insert Financial Institution Here]  Signature Card |

# **APPENDIX D**

**Internal New Account Request**

**Name of Business/Entity\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Nature of Business\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Type of Account Reqested\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Purpose of Account\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Description of anticipated activity, including check writing, ACH, domestic and international wire transfer volume:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Any additional services requested, online banking, online domestic wire transfer, Business Debit Card:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Requested by:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signature Date**

**Relationship Manager\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **APPENDIX E**

**HIGH- AND MEDIUM-RISK INDUSTRIES LIST**

**High Risk Industries**

* Arms/Weapons Dealers – applies to clients engaged in the manufacture, sale or distribution of arms as well as agents, brokers or intermediaries in such activities
* Art and Antique Dealers
* Money Services Businesses
* Cash Intensive Businesses – any retail business whose transaction profile shows $25,000 or more in cash transactions (aggregate of deposits and withdrawals) per week
* Casinos and Other Gaming or Wagering Establishments – these are always high-risk, even if they are reputable and publicly traded entities
* Charities, Endowments or Foundations – especially for organizations that accept funds from the public/third parties. Exceptions not considered high-risk include large, well known reputable organizations such as the March of Dimes, United Way, and the Red Cross, organizations that administer U.S. Government sponsored programs, such as the Fullbright Scholarship program, and Charities, Endowments or Foundations that use funds from an individual, family, school, etc., where the source of funds is clearly bona fide and third-party donations are not accepted.
* Deposit Brokers
* Embassies, Consulates or Ministries
* Third-party payment processors
* Privately-owned ATM machines
* Import/Export Brokers – those who never take possession of goods and/or have no physical location to demonstrate business
* Leather Goods Stores
* Off-Shore Personal Investment Companies, Money Management Businesses or Investment Management Businesses
* Businesses That Accept Third-Party Checks – third party checks are checks made payable to one party and deposited into an account of a differently named party. This does not include industries, such as collection agencies, where such conduct is not indicative of potential money laundering
* Professional Service Providers acting in an intermediary capacity, such as a lawyers’ trust account (IOLTA) or an escrow account, where the Bank has no direct relationship with or knowledge of the beneficial owners of the accounts
* Non-bank financial institutions that have accounts in the Private Wealth Management business. Examples include: securities/commodities firms, broker-dealers, mutual funds, hedge funds, commodity traders, investment advisors, dealers in precious metals, stones or jewels, pawnbrokers and loan or finance companies

**Medium Risk Industries**

* Import/Export Businesses – also referred to as wholesale/distribution businesses which ship abroad or receive physical inventory from outside the U.S. and maintain a store or warehouse that can be observed
* Internet Businesses – any business that sells goods and services over the Internet

# **APPENDIX F**

**MEDIUM-RISK PRODUCTS LIST**

The following products and services are deemed medium-risk:

* Remote Deposit Capture Service – Product that enables business customers to make check deposits via an electronic check conversion service.

# **APPENDIX G**

**STANDARD ACCOUNT REVIEW SHEET**

***To****:* Chief Executive Officer

***From****:*

***Date****:*

***Re****:* High – Risk Customer Submission

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Customer Information | | | | | | | | | | | | |
| **C****ustomer Name:** |  | | | | | | | | | | **New Customer** | |
| **Existing Customer** | |
| **Select the reason for the risk rating:** | | | **Note the risk rating: High** | | | | | | **Account Opening Date:** | | | |
| **PEP/SFPF**  **Geography**  **Industry**  **Product/Service**  **Transactions** | **Negative Information**  **Hedge Fund**  **Other:** | | | | | **Risk Rating Details:** | | | | | | |
|  | | | | | | |
| If customer is non-individual, list name(s) of owner(s): | | | | | |  | | | | | | |
| **C****ustomer’s/owner’s occupation/type of business:** | | | | | |  | | | | | | |
| The date that the account was placed on the High Risk List: | | | | | | | | | | | |  |
| Is owner related to other accounts? | | | | | | | | | | | | **Yes**  **No** |
| **Customer description/source of wealth/business operations information (including primary trade areas and major customers/suppliers):** | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
| Anticipated Monthly Sales/Income: (for non-individuals) | | | | |  | | | | | | | |
| Is customer’s residence/employment/business within reasonable proximity to the CRB office? | | | | | | | | | | | | Yes  No |
| If “No”, please explain: | |  | | | | | | | | | | |
| Is customer a home-based business or does he/she own/operate a home-based business? | | | | | | | | | | | | Yes  No |
| If “Yes”, please explain: | |  | | | | | | | | | | |
| Account Information | | | | | | | | | | | | |
| (Please include all accounts associated with the high-risk customer.) | | | | | | | | | | | | |
| **Account Name** | | Account Number | | | Product Type | | | **Account Purpose** | | | | |
|  | |  | | |  | | |  | | | | |
|  | |  | | |  | | |  | | | | |
|  | |  | | |  | | |  | | | | |
| Source of Initial Funding: | | | | |  | | | | | | | |
| Expected Monthly *Cash* Transaction Volumes: | | | | | In: | | | | | Out: | | |
| Enhanced Due Diligence (EDD) | | | | | | | | | | | | |
| **D****ate of Most Recent Customer Visit**  (Face-to-face meeting for individuals; site visit for non-individuals) | | | |  | | | | | | | | |
| **Was Internet search performed, Lexis Nexis report obtained, website viewed?** | | | | **Yes** (Please attach)  **No** | | | | | | | | |
| **Was any other EDD performed?** | | | | **Yes** (Please attach) **No** | | |  | | | | | |
| **Describe results of above efforts:** | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Privately Owned ATMs | | | | | | | |
| **Have you seen the contract between our customer and the ATM Service provider?**  **Yes**  **No** | | | | | | | |
| **How many ATMs does our customer own/operate: \_\_\_\_\_\_** (attach a listing of the addresses/locations of the ATMs**)** | | | | | | | |
| **What is the aggregate weekly currency usage for the customer’s ATMs: $ \_\_\_\_\_\_\_\_\_\_\_\_\_** | | | | | | | |
| **Does CRB provide the currency for the customer’s ATMs?**  **Yes**  **No** | | | | | | | |
| **I****f “no”, please explain:** |  | | | | | | |
| **Charities, Endowments, and Foundations** | | | | | | | |
| **Organizational Structure:**  **Corporation**  **Unincorporated Assoc/Club**  **Other** | | | | | | | |
| **I****f “Other: describe:** |  | | | | | | |
| **Geographic Area Served:** | |  | | | | | |
| **Is this organization affiliated with any other group(s):**  **Yes**  **No** | | | | | | | |
| **If “Yes”, please provide name(s)**  **of other group(s):** | | |  | | | | |
| **Source of Funding:**  **Private Donations**  **Sponsoring Corporation**  **Grants**  **Other** | | | | | | | |
| **I****f “Other: describe** |  | | | | | | |
| **Usage/Disbursement of Funds: Describe how and to whom funds will be paid:** | | | | | | | |
| **Subsequent Periodic Reviews** | | | | | | | |
| Describe any obvious changes in the account’s purpose: | | | | | | | |
|  | | | | | | | |
| Describe results of transaction activity review: | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| Approvals | | | | | | | |
|  | | | |  |  |  |  |
| **Relationship Officer** | | | |  | **Signature** |  | **Date** |
|  | | | |  |  |  |  |
| **CEO** | | | |  | **Signature** |  | **Date** |

# **APPENDIX H**

**RESPONSES TO INFORMATION REQUESTS**

According to Bank Policy, the BSA/AML Compliance Officer has been designated as the central Point of Contact for all 314(a) requests sent by FinCEN to the Bank.

FinCEN posts on its secure website a list of individuals, entities and organizations which are under investigation by one or more federal agencies. All financial institutions covered by 314(a) of the USA Patriot Act are required to quickly search their records to determine whether they maintain or have engaged in transactions with any of the named subjects.

If the Bank finds a match with a subject named on FinCEN’s 314(a) list, the match must be reported to FinCEN by making an entry on FinCEN’s secure website no later than fourteen (14) calendar days after the list was posted. At that point, a federal agency may follow up with a subpoena for specified documents. That subpoena is processed like any other subpoena from law enforcement. If the Bank has no match, no response is necessary.

A search of all pertinent Bank systems that contain customer information to determine whether or not the Company has any “hits” for the names listed on the request. The appropriate affirmative responses are entered on the FinCEN secure website.

Also the pertinent account or transactional activity is analyzed, and if the filing of a SAR is warranted, a SAR is prepared and filed.

All Bank employees involved in the processing and handling of 314(a) requests are required to keep the information confidential. The fact that a 314(a) request has been made, or that responsive information has been found, may not be shared with anyone outside of the Bank, with the exception of FinCEN and appropriate law enforcement officers. Moreover, the 314(a) requests and any supporting documentation must be maintained in secure files.

*Note: Refer to “314(a) Scanning Procedures” for detailed procedures regarding the process of down/up loading of files for filtering.*

# **APPENDIX I**

**POSSIBLE SIGNS OF ELDER FINANCIAL EXPLOITATION**

* 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
* 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.