CARRINGTON RIDGE, INC
Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

UPDATED AS OF JUNE 16, 2025

This document describes our Anti-Money Laundering (AML) Program as required by the Bank Secrecy Act (BSA) and its implementing regulations.

The firm's AML program implementation is "risk-based." That means that the program's AML policies, procedures and internal controls are designed to address the risk of money laundering specific to the firm. The firm can identify that risk by looking at the type of customers it serves, where its customers are located, and the types of services it offers. We have developed written analysis of our firm's money laundering and terrorist financing risk and how the firm's AML procedures manage that risk. This "risk-assessment" helps us to ensure that the AML program is the right one for the firm and is a useful tool for demonstrating to our examiners that we used a reasonable approach for designing our AML program.

In addition, where certain AML rules may be inapplicable due to the limited nature of the firm's business, FinCEN expects the firm to have internal controls in place to identify when circumstances change in such a way as to trigger previously inapplicable AML requirements and to amend our AML policies and procedures to accurately reflect all AML requirements that are applicable to our company. The firm is expected to identify and develop procedures for any additional AML requirements that do apply (*e.g.*, suspicious activity monitoring and reporting).

We will consult the websites maintained by the Financial Crimes Enforcement Network (FinCEN) and FINRA, including OFAC Sanctions Screening, for additional information and guidance. In order to submit BSA filings, including Suspicious Activity Reports (SARs), to FinCEN, the firm will use FinCEN's BSA E-Filing System.

1. Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities

by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely used in international cross border payments, cross border payments have risks that are conducive to the laundering of funds obtained elsewhere, as well as terrorist financing, that must be monitored and prevented.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AMLCompliance Person Designation and Duties

The firm shall designate a Anti-Money Laundering Program Compliance Person (AML Compliance Person), with responsibility for the firm’s AML program. The AML Compliance person has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including. The duties of the AML Compliance Person will include monitoring the firm’s compliance with AML obligations, overseeing

communication and training for employees, and maintaining all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

The firm will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate our Compliance Officer to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we are required to search those documents outlined in FinCEN's FAQ. If we find a match, the Compliance Officer will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), the Compliance Officer will structure our search accordingly.

If the Compliance Officer searches our records and does not find a matching account or transaction, then the Compliance Officer will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search including by: printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System, confirming that the firm has searched the 314(a) subject information against your records, maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

The firm will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

FinCEN also provides financial institutions with General Instructions and Frequently Asked Questions relating to 314(a) requests through the 314(a) Secured Information Sharing System or by contacting FinCEN's Regulatory Helpline at (800) 949-2732 or via email at sys314a@fincen.gov.

b. National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of money transmitters. ***NSLs are highly confidential. No officer, employee or agent can disclose to any person that a government authority or the FBI has sought or obtained access to records. We have policies and procedures in place for processing and maintaining the confidentiality of NSLs.***

The firm understands that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by ensuring that if we file a SAR after receiving that NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resource: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005).

c. Grand Jury Subpoenas

Grand juries may issue subpoenas as part of their investigative proceedings. The receipt of a grand jury subpoena does not in itself require the filing of a Suspicious Activity Report (SAR). However, money transmitters should conduct a risk assessment of the customer who is the subject of the grand jury subpoena, as well as review the customer's account activity. If suspicious activity is uncovered during this review, money transmitters should consider elevating the risk profile of the customer and file a SAR in accordance with the SAR filing requirements. Grand jury proceedings are confidential,

and a money transmitter that receives a subpoena is prohibited from directly or indirectly notifying the person who is the subject of the investigation about the existence of the grand jury subpoena, its contents or the information used to reply to it. If the firm files a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of it. The SAR will provide detailed information about the facts and circumstances of the detected suspicious activity.

The firm understands that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena through a confidential internal process, as designated by our Compliance Officer. If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resources: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006).

d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

BSA regulations permit financial institutions to share information with other financial institutions under the protection of a safe harbor if certain procedures are followed. The firm shares or plans to share information with other financial institutions, and this section describes the firm's procedures for such sharing.

The firm will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. The Compliance Officer will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. The firm will use the notice form found at FinCEN's website. Before the firm shares information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. The firm understands that this requirement applies even to financial institutions *with which we are affiliated*, and that we will obtain the requisite

notices from affiliates and follow all required procedures.

The firm will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.

The firm will also employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

Resources: FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (6/16/2009).

4. Checking the Office of Foreign Assets Control Listings

Although not part of the BSA and its implementing regulations, the Office of Foreign Assets Control (OFAC) compliance is often performed in conjunction with AML compliance. OFAC is an office of the U.S. Treasury that administers and enforces economic sanctions and embargoes based on U.S. foreign policy and national security goals that target geographic regions and governments (e.g., Cuba, Sudan and Syria), as well as individuals or entities that could be anywhere (e.g., international narcotics traffickers, foreign terrorists and proliferators of weapons of mass destruction). As part of its enforcement efforts, OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list), which includes names of companies and individuals who are connected with the sanctions targets. U.S. persons are prohibited from dealing with SDNs wherever they are located, and all SDN assets must be blocked. Because OFAC's programs are constantly changing, describe how you will check with OFAC to ensure that your SDN list is current and also that you have complete information regarding the listings of economic sanctions and embargoes enforced by OFAC affecting countries and parties before opening an account and for existing accounts.

Before opening an account, and on an ongoing basis, the Compliance will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (*See* the OFAC website for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any

available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. *See also* FINRA's OFAC Search Tool that screens names against the SDN list. The Compliance Officer will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and will document the review.

If the firm determines that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve international money transmission activities.

5. Customer Identification Program

The Firm has and follows reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures address the types of information the firm will collect from the customer and how it will verify the customer's identity. These procedures enable the firm to form a reasonable belief that it knows the true identity of its customers. The firm's customer identification program (CIP) is in writing and is part of the firm's AML compliance program.

The firm has established, documented and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government. *See* Section 5.g. (Notice to Customers) for additional information.

a. Required Customer Information

Allowed customers of the firm are US incorporated entities only. This includes limited liability companies (LLCs), limited partnerships (LPs), and Corporations, with verified Employment Identification Numbers (EINs). No unincorporated US companies that use SSNs in lieu of EINs will be accepted. Offshore or other non-US incorporated entity types can be approved by exception, but must have a US bank account.

Prior to opening an account, the firm will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

1. First and Last Name of Person with Significant Control (PSC). This person should be a Business Officer with the business title Manager, Member, Managing Partner, Owner, CEO, or President.

2. Email address and US phone number of the PSC
3. Date of birth of the PSC, mm/dd/yyyy
4. Physical or Mailing Address of PSC
5. First and Last Name of all Ultimate Beneficial Owners (UBOs). A UBO is defined as an individual with 25% or higher ownership share in the business.
6. Date of birth of the UBOs, mm/dd/yyyy
7. Physical or Mailing Address of UBOs
8. For all UBOs and PSCs: a US tax identification number, such as a social security number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).
9. For all UBOs and PSCs: Copies of an official US identification document including a US passport, drivers license, or Social Security Card
10. US entity name. Must be an incorporated LLC, LP, or Corporation.
11. Abusiness address, which will be a business street address or a principal place of business, local office, or other physical location; and
12. An IRS Employer Identification Number (EIN) for the US entity, with the IRS EIN letter
13. Business Banking routing and account number. A banking statement from the most recent statement cycle should also be provided.
14. Written description about business activities and expected purpose and amount of transactions

For exceptions: when opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be

notified so that we can determine whether we should report the situation to FinCEN on a SAR.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The Compliance Officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

The firm will verify customer identity through documentary means, non-documentary means or both. The Firm will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, the firm will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. The firm may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, the firm will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For an entity, showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

The firm will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer

reporting agency, public database or other source
- Checking references with other financial institutions; or
- Obtaining a financial statement.

The firm will use non-documentary methods of verification when:
- the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- the firm is unfamiliar with the documents the customer presents for identification verification;
- the customer and firm do not have face-to-face contact; and
- there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

The firm will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

The firm recognizes that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. The firm will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

e. Recordkeeping

The firm will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made. The firm will maintain an electronic database for all corporate records, transactions, and applications from prospective customers.

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list 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. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers

The CIP Rule requires our firm to provide adequate notice to customers that you are requesting information from them to verify their identities. We provide such notice through written, online, or telecommunication notice.

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: email or in-person.

Important Information About Procedures for Opening a New Account

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

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

Rule: 31 C.F.R. § 1023.220(a)(5).

h. Reliance on Another Financial Institution for Identity Verification

The firm may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with the firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

Note: We will not be held responsible for the failure of the other financial institution to fulfill adequately their CIP responsibilities, provided that we can establish that our reliance was reasonable and that we have obtained the requisite contracts and certifications.

6. Customer Due Diligence Rule

On May 11, 2016, FinCEN adopted a final rule on Customer Due Diligence Requirements for Financial Institutions (CDD Rule) to clarify and strengthen customer due diligence for covered financial institutions. The Rule became effective on May 11, 2018.

In its CDD Rule, FinCEN identifies four components of customer due diligence: (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (4) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. As the first component is already an AML program requirement (under the CIP Rule), the CDD Rule focuses on the other three components.

Specifically, the CDD Rule focuses particularly on the second component by adding a

new requirement that covered financial institutions establish and maintain written procedures as part of their AML programs that are reasonably designed to identify and verify the identities of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.

Under the CDD Rule, financial institutions must obtain from the natural person opening the account on behalf of the legal entity customer, the identity of the beneficial owners of the entity. In addition, that individual must certify, to the best of his or her knowledge, as to the accuracy of the information. FinCEN intends that the legal entity customer identifies its ultimate beneficial owner(s) and not "nominees" or "straw men."

The CDD Rule does not prescribe the form in which financial institutions must collect the required information, which includes the name, date of birth, address and Social Security number or other government identification number of beneficial owners. Rather, member firms may choose to obtain the information by using FinCEN's standard certification form in Appendix A of the CDD Rule (at https://www.fincen.gov/resources/filing-information) or by another means, provided that the chosen method satisfies the identification requirements in the CDD Rule. In any case, the CDD Rule requires that member firms maintain records of the beneficial ownership information they obtain.

Once the firm obtains the required beneficial ownership information, the CDD Rule requires that firms verify the identity of the beneficial owner(s) – in other words, that they are who they say they are – and not their status as beneficial owners through risk-based procedures that include, at a minimum, the elements required for CIP procedures for verifying the identity of individual customers. Such verification must be completed within a reasonable time after account opening. Member firms may rely on the beneficial ownership information supplied by the individual opening the account, provided that they have no knowledge of facts that would reasonably call into question the reliability of that information.

The CDD Rule's requirements with respect to beneficial owners of legal entity customers apply on a prospective basis, that is, only with respect to legal entity customers that open new accounts from the date of the CDD Rule's implementation. However, member firms should obtain beneficial ownership information for an existing legal entity customer if, during the course of normal monitoring, it receives information that is needed to assess or reevaluate the risk of the customer.

The required records to be created and maintained must include: (i) for identification, any identifying information obtained by the member firm pursuant to the beneficial ownership identification requirements of the CDD Rule, including without limitation the certification (if obtained); and (ii) for verification, a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of

issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and the resolution of each substantive discrepancy.

The firm may rely on the performance by another financial institution (including an affiliate) of the requirements of the CDD Rule with respect to any legal entity customer of the member firm that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that: (1) such reliance is reasonable under the circumstances; (2) the other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and (3) the other financial institution enters into a contract requiring it to certify annually to the member firm that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the member firm's procedures to comply with the CDD Rule.

The CDD Rule also addresses the third and fourth components, which FinCEN states "are already implicitly required for covered financial institutions to comply with their suspicious activity reporting requirements," by amending the existing AML program rules for covered financial institutions to explicitly require these components to be included in AML programs as a new "fifth pillar." These requirements are discussed further below.

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)
Resources: 81 Fed. Reg. 29398 (May 11, 2016) (Final Rule: Financial Crimes Enforcement Network; Customer Due Diligence Requirements for Financial Institutions); FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40; FIN-2018-G001: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (4/3/2018); Regulatory Notice 18-19.

The firm has established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers.[1] We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

a. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, the firm will identify any individual that is a beneficial owner of the legal entity customer by identifying any

individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), or an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
(4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

---

[1] Beneficial owners and legal entity customers as defined by the CDD Rule.

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

Rules: 31 C.F.R. § 1010.230(b); 31 C.F.R. § 1023.210(b)(5).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016)

b. Understanding the Nature and Purpose of Customer Relationships

FinCEN states that the CDD Rule requires that firms must necessarily have an understanding of the nature and purpose of the customer relationship in order to determine whether a transaction is potentially suspicious and, in turn, to fulfill their SAR obligations. To that end, the CDD Rule requires that firms understand the nature and purpose of the customer relationship in order to develop a customer risk profile. The customer risk profile refers to information gathered about a customer to form the baseline against which customer activity is assessed for suspicious transaction reporting. Information relevant to understanding the nature and purpose of the customer relationship may be self-evident and, depending on the facts and circumstances, may include such

information as the type of customer, account or service offered, and the customer's income, net worth, domicile, or principal occupation or business, as well as, in the case of existing customers, the customer's history of activity. The CDD Rule also does not prescribe a particular form of the customer risk profile. Instead, the CDD Rule states that depending on the firm and the nature of its business, a customer risk profile may consist of individualized risk scoring, placement of customers into risk categories or another means of assessing customer risk that allows firms to understand the risk posed by the customer and to demonstrate that understanding.

The CDD Rule also addresses the interplay of understanding the nature and purpose of customer relationships with the ongoing monitoring obligation discussed below. The CDD Rule explains that firms are not necessarily required or expected to integrate customer information or the customer risk profile into existing transaction monitoring systems (for example, to serve as the baseline for identifying and assessing suspicious transactions on a contemporaneous basis). Rather, FinCEN expects firms to use the customer information and customer risk profile as appropriate during the course of complying with their obligations under the BSA in order to determine whether a particular flagged transaction is suspicious.

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile.

Depending on the facts and circumstances, a customer risk profile may include such information as:

- The type of customer;
- The account or service being offered;
- The customer's income;
- The customer's net worth;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(i).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016)

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

As with the requirement to understand the nature and purpose of the customer relationship, the requirement to conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial ownership of legal entity customers,

merely adopts existing supervisory and regulatory expectations as explicit minimum standards of customer due diligence required for firms'AML programs. If, in the course of its normal monitoring for suspicious activity, the firm detects information that is relevant to assessing the customer's risk profile, the firm must update the customer information, including the information regarding the beneficial owners of legal entity customers, as discussed above. However, there is no expectation that the firm will update customer information, including beneficial ownership information, on an ongoing or continuous basis.

The firm will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016)

7. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

The BSA, as amended by Section 312 of the USA PATRIOT Act, and the rules promulgated thereunder require, in part, that a firm, as part of its anti-money laundering program, establish a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the firm to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered or managed by the firm for a foreign financial institution.

Aforeign financial institution is:

(1) a foreign bank;
(2) any branch or office located outside the United States
(3) any person organized under foreign law (other than a branch or office of such person in the United States) that is engaged in the business of, and is readily identifiable as: (a) a currency dealer or exchanger; or (b) a money transmitter.

Aperson, however, is not "engaged in the business" of a currency dealer, a currency exchanger or a money transmitter if such transactions are merely incidental to the person's business.

A "correspondent account" is defined in this context as any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursement on behalf of, the foreign financial institution, or to handle other financial transactions for the foreign financial institution.

On January 30, 2008, FinCEN issued guidance clarifying that covered financial institutions presenting a negotiable instrument for payment to a foreign financial institution on which the instrument is drawn would not, by itself, be establishing a correspondent account between the covered financial institution and the paying institution. See FIN-2008-G001: Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment (1/30/2008).

The firm will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

If we have correspondent accounts for foreign financial institutions, we will assess the money laundering risk posed, based on a consideration of relevant risk factors. We can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors can include:

- the nature of the foreign financial institution's business and the markets it serves;
- the type, purpose and anticipated activity of such correspondent account;
- the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;
- the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and
- information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of

money laundering.

The firm will apply our risk-based due diligence procedures and controls to each financial foreign institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity.

b. Enhanced Due Diligence

The BSA, as amended by Section 312 of the USA PATRIOT Act, and the rules promulgated thereunder require, in part, that a firm's due diligence program for correspondent accounts of foreign financial institutions include the performance of enhanced due diligence on correspondent accounts for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering

concerns.

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (*e.g.*, using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a sub account, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of

stock in a foreign bank. We also understand that members of the same family shall be considered to be one person.

c. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

The firm has procedures for circumstances in which we cannot perform appropriate due diligence for a correspondent account of a foreign financial institution or the enhanced due diligence that is required for correspondent accounts for certain foreign banks.

In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR, close the correspondent account and/or take other appropriate action.

Rule: 31 C.F.R. § 1010.610(d).

9. Due Diligence and Enhanced Due Diligence Requirements for Senior Foreign Political Figures

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual widely and publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

The firm will do Politically Exposed Person (PEP) screening using third party databases. Senior foreign political figures will require special approval from our Compliance Officer and significant evidence of AML compliance in order to open an account with the firm. The firm does not open or maintain private banking accounts.

Rule: 31 C.F.R. § 1010.620.
Resources: Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption (1/1/2001); FIN-2008-G005: Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Political Corruption (4/17/2008).

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

The firm will comply with the BSA, as amended by Section 311 of the USA PATRIOT Act, which grants the Secretary of the Treasury the authority, after finding that reasonable grounds exist for concluding that (1) a jurisdiction outside of the United States; (2) one or more financial institutions operating outside of the United States; (3) one or more classes of transactions within, or involving, a jurisdiction outside of the United States; or (4) one or more types of accounts is of "primary money laundering concern," to require domestic financial institutions to take certain "special measures" against the primary money laundering concern. There is a special section on the FinCEN website where all the Section 311 designations are listed. See Section 311 – Special Measures.

If FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, the firm understands that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule. For example, if the final rule deems a certain bank and its subsidiaries (Specified Banks) to be of primary money laundering concern, a special measure may be a prohibition from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. In that case, the firm will take the following steps:

(1) We will review our account records, including correspondent account records, to ensure that our account holders and correspondent account holders maintain no accounts directly for, or on behalf of, the Specified Banks; and

(2) We will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against indirect use of those accounts by the Specified Banks. Such due diligence may include:

- Notification to Correspondent Account Holders

  We will notify our correspondent account holders that the account may not be used to provide the Specified Banks with access to us. We will transmit the notice to our correspondent accounts and we shall retain documentation of such notice.

- Identification of Indirect Use

  We will take reasonable steps in order to identify any indirect use of our correspondent accounts by the Specified Banks. We will determine if such indirect use is occurring from transactional records that we maintain in the normal course of business. We will take a risk-based approach when deciding what, if any, additional due diligence measures we should adopt to guard against the

indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, their correspondents.

We understand that we have an ongoing obligation to take reasonable steps to identify all correspondent account services our correspondent account holders may directly or indirectly provide to the Specified Banks.

Rules: 31 C.F.R. §§ 1010.651, 1010.653, 1010.655, 1010.658, 1010.659, 1010.660.
Resources: Section 311 – Special Measures (for information on all special measures issued by FinCEN).

11. Monitoring Accounts for Suspicious Activity

Money transmitters must establish risk-based procedures reasonably designed to detect and report suspicious transactions in order to comply with the BSA. These procedures must include using the customer's risk profile as a baseline to monitor for suspicious activity. The risk of suspicious activity will vary for each firm depending on its size and location and based on its business model and the products and services it offers. The firm can identify that risk by looking at the type of customers it serves, where its customers are located, and the types of products and services it offers. Given the wide variety of business models employed by small firms, it is paramount that the firm's monitoring procedures be tailored to the firm's business and identified risks. Additionally, your procedures should identify "red flags" or indicators of possible suspicious activity to identify circumstances warranting further due diligence by the firm. Higher risk accounts and transactions generally need to be subjected to greater scrutiny.

These procedures describe how the firm will monitor for or otherwise identify these "red flags." The firm may monitor transactions manually or through automated systems or a combination of the two, as long as the system is reasonably designed to identify and report suspicious activity. Note that the types of suspicious activity that are reportable on a SAR are very broad.

The firm will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) Monitoring will be conducted through automated and manual methods. These procedures will include a list of reports as well as their purpose and description. If manual monitoring is utilized, these procedures will include a list of documents/systems to be reviewed and the purpose of the review. Regardless of the method, these procedures will address how this monitoring will be conducted and the frequency with which it will be conducted. The customer risk profile

will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee. The Compliance Officer will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

The firm will conduct reviews of activity of our monitoring system and detection efficacy. The firm will document our monitoring and reviews. The AML Compliance Officer or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed.

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office, and local FBI office. If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR.

Rule: 31 C.F.R. § 1023.320.
Resources: *FinCEN's website*; *OFAC web page*

b. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Potential Red Flags in Customer Due Diligence and Interactions with Customers

- The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
- The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior

financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.

- The customer refuses to identify a legitimate source of funds or information that is false, misleading or substantially incorrect.
- The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).
- The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
- The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
- The customer's background is questionable or differs from expectations based on business activities.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
- An account is opened by a politically exposed person (PEP),[9] particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company[10] beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
- An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.[11]

- An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.[12]
- An account is opened in the name of a foreign financial institution, such as an offshore bank
- An account is opened for a foreign financial institution that is bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

Potential Red Flags in Money Movements

- The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
- The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
- The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
- The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.
- The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Incoming payments are made by third-party checks or checks with multiple endorsements.
- Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
- Payments are made by third party check or money transfer from a source that has no

apparent connection to the customer.

- Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.

- Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.

- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).

- The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.

- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.

- There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.

- The account is used for payments or outgoing wire transfers with little or no relevant purpose (*i.e.*, the account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).

- Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

- The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.

- The customer uses a personal/individual account for business purposes or vice versa.

- A foreign import business with U.S. accounts receives payments from outside the area of its customer base.

- There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
- Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the

descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).

- The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.

- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

- A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).

- Nonprofit or charitable organizations engage in financial transactions 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.

- There is unusually frequent domestic and international automated teller machine (ATM) activity.

- Aperson customarily uses the ATM to make several deposits below a specified BSA/AML reporting threshold.

- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.

- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

Other Potential Red Flags

- The customer is reluctant to provide information needed to file reports to proceed with the transaction.

- The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.

- The customer tries to persuade an employee not to file required reports or not to maintain the required records.
- Law enforcement has issued subpoenas or freeze letters regarding a customer or

account at a financial institution.

- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.

- The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.

- The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.

- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

- The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.

- The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).

- There is an unusual use of trust funds in business transactions or other financial activity.

c. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the Compliance Officer *for escalation of suspicious activity*. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR.

12. Suspicious Transactions and BSA Reporting

The firm's procedures are meant to identify any suspicious transactions and determine if they need further investigation or warrant filing a SAR. These procedures cover the maintenance of SAR documentation and the preservation of its confidentiality, and BSA reporting. The firm exercises due diligence in monitoring suspicious activity as the regulations require us to file a SAR when we "know, suspect, or have reason to suspect" that transactions involve certain suspicious activities.

The firm exempts from reporting on a SAR the following violations: (1) a robbery or burglary that is committed or attempted and already reported to appropriate law enforcement authorities; If the firm relies on one of these exemptions, it may be required

to demonstrate that we relied on one of these exemptions and must maintain records, for at least five years, of our determination not to file a SAR based on the exemption.

Rule: 31 C.F.R. § 1023.320.
Resources: FinCEN's BSA E-Filing System.

a. Filing a SAR

The firm will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through the firm involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
(4) the transaction involves the use of the firm to facilitate criminal activity.

The firm will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

The firm may file a voluntary SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

The firm will report suspicious transactions by completing a SAR, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not

mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

The firm will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state regulators upon request.

The firm will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by FinCEN or another appropriate law enforcement or regulatory agency, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

Rules: 31 C.F.R. § 1023.320
Resources: FinCEN's website contains additional information, including information on the BSA E-Filing System, the FinCEN Suspicious Activity Report: Introduction and Filing Instructions, and the biannual SAR Activity Review – Trends, Tips & Issues, which discusses trends in suspicious reporting and gives helpful tips; The SAR Activity Review, Issue 10 (May 5/2006) (documentation of decision not to file a SAR; grand jury subpoenas and suspicious activity reporting, and commencement of 30-day time period to file a SAR); FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007); NTM 02-21; NTM 02-47.

b. Currency Transaction Reports

A firm must file a currency transaction report (CTR) for each deposit, withdrawal, exchange of currency, or other payment or transfer by, through or to the firm that involves a transaction in currency of more than $10,000 or for multiple transactions in currency of more than $10,000 when a financial institution knows that the transactions are by or on behalf of the same person during any one business day, unless the transaction is subject to certain exemptions. "Currency" is defined as "coin and currency of the United States or of any other country" that is "customarily used and accepted as money in the country in which issued; and a cashier's check (by whatever name called, including 'treasurer's check' and 'bank check'), bank draft, traveler's check, or money order having a face amount of not more than $10,000 received in a designated reporting transaction . . . or received in any transaction in which the recipient knows that such monetary instrument is

being used in an attempt to avoid the reporting of the transaction."

The firm prohibits transactions involving physical currency and has the following procedures to prevent such transactions. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the *BSA E-Filing System* to file the supported CTR Form.

Rules: 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.
Resource: FinCEN's BSA E-Filing System (including instructions for FinCEN CTR Form 112).

c. Currency and Monetary Instrument Transportation Reports

A currency and monetary instrument transportation report (CMIR) must be filed whenever more than $10,000 in currency or other monetary instruments is physically transported, mailed or shipped into or from the United States. A CMIR also must be filed whenever a person receives more than $10,000 in currency or other monetary instruments that has been physically transported, mailed or shipped from outside the United States and a CMIR has not already been filed with respect to the currency or other monetary instruments received. ACMIR is not required to be filed by a financial institution mailing or shipping currency or other monetary instruments through the postal service or by common carrier. "Monetary instruments" include the following: currency (defined above); traveler's checks in any form; all negotiable instruments (including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in such form that title passes upon delivery; incomplete negotiable instruments that are signed but omit the payee's name; and securities or stock in bearer form or otherwise in such form that title passes upon delivery.

The firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal

service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN's website.

Rules: 31 C.F.R. §§ 1010.340, 1010.306.
Resources: FinCEN's BSA E-Filing System.

d. Foreign Bank and Financial Accounts Reports

The regulations under the BSA require financial institutions such as money transmitters to report and keep records related to any financial interest in, or signature authority over, a bank account or other financial account that the firm has in a foreign country in which the aggregate value of any accounts exceed $10,000.

The firm will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than $10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the BSA E-Filing System provided on FinCEN's website.

Rules: 31 C.F.R. §§ 1010.306, 1010.350, 1010.420.
Resources: FinCEN's BSA E-Filing System.

e. Monetary Instrument Purchases

No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 to $10,000 inclusive in currency unless it obtains and records certain information when issuing or selling one or more of these instruments to any individual purchaser. A financial institution issuing or selling one or more of these instruments to any individual purchaser in excess of $10,000 will also need to file a CTR. See Section 12.b.

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more.

f. Funds Transmittals of $3,000 or More Under the Travel Rule

When we are the transmitter's financial institution in funds of $3,000 or more, we will retain either the original or a copy (*e.g.*, microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmitter; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient's financial institution. In addition,

we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmitter is not an established customer of the firm (*i.e.,* a customer of the firm who has not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance). If a transmitter or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (*e.g.,* driver's license); and (3) the person's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If a transmitter or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the method of payment (*e.g.,* check or credit card transaction). In the case of transmitters only, we shall also obtain the transmitter's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

13. AMLRecordkeeping

a. Responsibility for Required AML Records and SAR Filing

The firm has procedures to maintain all applicable AML program records and reviews.

Our AML Compliance Officer and his or her designee will be responsible for ensuring that AML records are maintained properly and that SARs are filed as required.

In addition, as part of our AML program, the firm will create and maintain SARs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transmittals. We will maintain SARs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements for no less than five years.

b. SAR Maintenance and Confidentiality

The firm will hold SARs and any supporting documentation confidential. We will not

inform anyone outside of FinCEN or other appropriate law enforcement or regulatory agencies about SARs. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. *See* Section 11 for contact numbers. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Person will handle all subpoenas or other requests for SARs. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

c. Additional Records

The firm is required to retain either an original or a microfilm or other copy or reproduction of certain records.

We shall retain either the original or a microfilm or other hard copy or reproduction of each of the following, as needed:

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;

- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks of more than $10,000 to or from any person, account or place outside the U.S.;

- Arecord of each advice, request or instruction given to another financial institution or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks of more than $10,000 to a person, account or place outside the U.S.;

- Each document granting signature or trading authority over each customer's account;

- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments of more than $10,000 to a person, account or place, outside the U.S.; and

- Arecord of each receipt of currency, other monetary instruments, checks of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

These physical documents will be stored in a safe and secure location, as determined by our Compliance Officer.

14. Privacy Policies

The firm will work closely with other financial institutions to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with our contractual obligations and with AML laws. Both the firm and any third party financial institutions will file the necessary annual certifications for such information sharing, which can be found on FinCEN's website. As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity, identify reports, and the manner in which they will be used. We will provide third party financial institutions with proper customer identification and due diligence information as required to successfully monitor customer transactions. We will describe how each financial institution will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

15. Training Programs

This section describes our AML ongoing employee training and programs.

The firm will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on the firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

The firm will develop internal training, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

The firm will review its operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our

written procedures will be updated to reflect any such changes.

Rules: 31 CFR § 1023.210(b)(4).
Resources: See FinCEN SAR Narrative Guidance Package (11/01/2003); FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007).

16. Program to Independently Test AML Program

The firm will decide on an annual basis whether to independently test our AML program with firm personnel or a qualified outside party who could perform this function. This independent AML program testing will be performed annually (on a calendar year basis). In some instances, an independent test could occur every two calendar years depending on risk levels. All firms should undertake more frequent testing than required if circumstances warrant.

The independent testing of the firm's AML compliance program will include: (1) evaluating the overall integrity and effectiveness of our AML compliance program; (2) evaluating our procedures for BSA reporting and recordkeeping requirements; (3) evaluating the implementation and maintenance of our CIP; (4) evaluating our customer due diligence requirements; (5) evaluating our transactions, with an emphasis on high-risk areas; (6) evaluating the adequacy of our staff training program; (7) evaluating our systems, whether automated or manual, for identifying suspicious activity; (8) evaluating our systems for reporting suspicious activity; (9) evaluating our policy for reviewing accounts that generate multiple SAR filings; and (10) evaluating our response to previously identified deficiencies.

a. Staffing

The testing of our AML program will be performed at least annually by an independent third party, or other third party as designated by our Compliance Officer. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management or to an internal audit committee. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

17. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by a member of the senior management team.

18. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to the president/chairman of the board/audit committee chair. Such reports will be confidential, and the employee will suffer no retaliation for making them.

19. Additional Risk Areas

This AML Compliance Manual and any amendments must be approved and signed off on by the Company's Board of Directors and Compliance Officer.

Prohibited Countries/Jurisdictions :

Afghanistan, Belarus, Bosnia and Herzegovina, Burma (Myanmar), Central African Republic, the Democratic Republic of Congo, Croatia, Cuba, Ethiopia, Iran, Iraq, Kosovo, Lebanon, Libya, Macedonia (North), Mali, Montenegro, Nicaragua, North Korea, Russian Federation, Serbia, Slovenia, Somalia, South Sudan, Sudan, Syria, Ukraine, Venezuela, Yemen, Zimbabwe

Prohibited Industries/Sectors:

Gambling, Marijuana/cannabis related businesses, Guns, Arms and ammunition, Precious metals services, Adult entertainment or Pornography.

Prohibited Customers:

Politically Exposed Persons (PEPs)

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. We do not believe there are any additional risk areas.

20. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor the firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below, including the Board of Directors.

Signed: _____

Name: _____

Title: Chief Compliance Officer

Date: _____

Signed: _____

Name: _____

Title: _____

Date: _____