

Integrity Trade LLC

Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

UPDATED AS OF FEBRUARY 06, 2024

IMPORTANT LINKS

The [FINRA AML web page](#) includes important information and links to other websites with useful information. You should also consult the websites maintained by the [Financial Crimes Enforcement Network \(FinCEN\)](#) and the [Securities and Exchange Commission \(SEC\)](#), including the [SEC's AML Source Tool](#), for additional information and guidance. For historical guidance and background, you may wish to consult NASD Notices to Members (NTM) [02-21](#), [02-47](#), [02-50](#), [02-78](#), [02-80](#), [03-34](#), [06-07](#), [06-41](#) and [07-17](#). Regulatory Notices [07-42](#), [08-66](#), [09-05](#), [12-08](#), [17-40](#) [18-19](#), and [19-18](#) provide additional guidance information about firms' AML obligations. In order to submit BSA filings, including Suspicious Activity Reports (SARs), to FinCEN, firms must use FinCEN's [BSA E-Filing System](#).

1. Firm Policy For Integrity Trade LLC

It is the policy of Integrity Trade LLC is 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 deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit

funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

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 and FINRA rules and 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.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

Designate your firm's AML Compliance Person and describe his or her duties.

The firm has designated Christian Raburn as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Christian Raburn has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including Completing ICC Academy and scoring 99%. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and [add any other duties your firm will assign to the AML Compliance Person; review NASD Rules 1021 and 1031¹ for any applicable registration requirements]. The AML Compliance Person will also ensure that the firm keeps and maintains 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. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person through the FINRA Contact System (FCS), including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). The firm will promptly notify FINRA of any change in this information through FCS and will review,

¹ As of October 1, 2018, NASD Rules 1021 and 1031 will no longer be effective. As of October 1, 2018, see FINRA Rule 1210.

and if necessary update, this information within 17 business days after the end of each calendar year. The annual review of FCS information will be conducted by Christian Raburn and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, Christian Raburn will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310; FINRA Rule 4517.

Resources: [Regulatory Notice 07-42](#); [NTM 06-07](#); [NTM 02-78](#). Firms can submit their AML Compliance Person information through [FINRA's FCS web page](#).

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

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

Pursuant to the BSA and its implementing regulations, financial institutions are required to make certain searches of their records upon receiving an information request from FinCEN. Describe your firm's procedures for FinCEN requests for information on money laundering or terrorist activity.

In order for a firm to obtain information requests from FinCEN, the firm must first designate an AML Contact Person in FCS. You should be aware that if you want to change the person who receives FinCEN requests, you must change the AML contact information in FCS. When you are faced with a change in personnel who will receive this information, you should be aware that FinCEN receives a data feed of this revised information from FCS every other week and that it may take several weeks for a firm's new AML contact person to receive information from FinCEN. Therefore, it is advisable for a firm that is aware that a person who had been receiving FinCEN requests is leaving the firm to change the information on FCS as soon as practical to ensure continuity of receiving FinCEN information.

We 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 through the FINRA Contact System (FCS) one or more persons 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, Christian Raburn

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), Christian Raburn will structure our search accordingly.

If Christian Raburn searches our records and does not find a matching account or transaction, then Christian Raburn will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by [*add the details on how your firm will document its searches here. For example, printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System confirming that your firm has searched the 314(a) subject information against your records OR 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. Christian Raburn 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.

We 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.

Rule: 31 C.F.R. § 1010.520.

Resources: [FinCEN's 314\(a\) web page](#); [NTM 02-80](#); 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 broker-dealers. NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Firms that receive NSLs must have policies and procedures in place for processing and maintaining the confidentiality of NSLs. If you file a Suspicious Activity

Report (SAR) after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL.

We understand 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 [*describe procedure*]. If we file a SAR after receiving an 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, broker-dealers 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, broker-dealers 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 broker-dealer 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 you file a SAR after receiving a grand jury subpoena, the SAR should not contain any reference to the receipt or existence of it. The SAR should provide detailed information about the facts and circumstances of the detected suspicious activity.

We understand 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 by [*describe procedure*]. 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. If your firm shares or plans to share information with other financial institutions, describe your firm's procedures for such sharing.

We 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. Christian Raburn will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at [FinCEN's website](#). Before we share 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. We understand 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.

We 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 and [*describe any other procedures*].

We also will 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.

Rules: 31 C.F.R. § 1010.540.

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 \(6/16/2009\)](#).

e. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

The obligation to identify and properly report a suspicious transaction and to timely file a SAR rests separately with each broker-dealer. However, one SAR may be filed for a suspicious activity by all broker-dealers involved in a transaction (so long as the report filed contains all relevant and required information) if the SAR is jointly filed. In addition, if a broker-dealer and another financial institution that is subject to the SAR regulations are involved in the same suspicious transaction, the financial institution may also file a SAR jointly (so long as the report filed contains all relevant and required information). For example, a broker-dealer and an insurance company may file one SAR with respect to suspicious activity involving the sale of variable insurance products. Disclosures that are made for the purposes of jointly filing a SAR are protected by the safe harbor contained in the SAR regulations. The financial institutions that jointly file a SAR shall each be separately responsible for maintaining a copy of the SAR and should maintain their own SAR supporting documentation in accordance with BSA recordkeeping requirements. See generally Section 12 (Suspicious Transaction and BSA Reporting) for information on a broker-dealer's obligation to file a SAR to report suspicious transactions.

We will file joint SARs in the following circumstances, according to [*describe procedures*]. We will also share information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR.

[If an introducing firm:] We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a SAR. In cases in which we file a joint SAR for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR.

If we determine it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly (*e.g.*, because the SAR concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R. § 1010.430; 31 C.F.R. § 1010.540.

Resources: FinCEN's [BSA E-Filing System](#).

f. Sharing SARs With Parent Companies

On January 20, 2006, FinCEN issued guidance permitting under certain conditions the sharing of SARs with either foreign or domestic parent entities.

Because we are a subsidiary, we may share SARs with [*Name of parent entity (or parent entities)*]. Before we share SARs with [*Name(s)*], we will have in place written confidentiality agreements or written arrangements that [*Name(s)*] protect the confidentiality of the SARs through appropriate internal controls.

[If parent company is a non-U.S. entity:] The confidentiality agreement will state that the recipient foreign parent entity (or entities) may not disclose further any SAR, or the fact that such report has been filed. The agreement will allow for the foreign parent entity (or entities) to disclose without permission underlying information (that is, information about the customers and transaction(s) reported) that forms the basis for the SAR and that does not explicitly reveal that a SAR was filed and that is not otherwise subject to disclosure restrictions.

Resource: FinCEN's [BSA E-Filing System](#), [FinCEN Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities \(1/20/2006\)](#).

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, Christian Raburn 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 [OFAC's Sanctions List Search](#) tool, which screens names against the SDN list and other sanctions lists administered by OFAC. Christian Raburn will also review existing accounts against

the SDN list and listings of current sanctions and embargoes when they are updated and [he or she] will document the review.

If we determine 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 physical security certificates or application-based investments (e.g., mutual funds).

Rules: 31 C.F.R. § 501.603; 31 C.F.R. § 501.604.

Resources: [SEC AML Source Tool for Broker-Dealers, Item 12](#); [OFAC Lists web page](#) (including links to the SDN List and lists of sanctioned countries); [OFAC's Sanctions Lists Search](#). You can also subscribe to receive updates on the [OFAC Subscription web page](#). See also the following [OFAC forms](#): [Report of Blocked Transactions Form](#); [Report of Rejected Transactions Form](#); [Annual Report of Blocked Property Form](#); and [OFAC Guidance Regarding Foreign Assets Control Regulations for the Securities Industry](#).

5. Customer Identification Program

Firms are required to have and follow reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures must address the types of information the firm will collect from the customer and how it will verify the customer's identity. These procedures must enable the firm to form a reasonable belief that it knows the true identity of its customers. The final rule, which FinCEN and the SEC jointly issued on April 30, 2003, applies to all new accounts opened on or after October 1, 2003.

The firm's customer identification program (CIP) must be in writing and be part of the firm's AML compliance program.

Note that the CIP rule applies only to "customers" who open new "accounts" with a broker-dealer. Specifically, the CIP rule defines a "customer" as (1) a person that opens a new account or (2) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. "Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well.

Also, for purposes of the CIP rule's definition of customer, the following entities are excluded from the definition of "customer":

- a financial institution regulated by a federal functional regulator (that is, an institution regulated by the Board of Governors of the Federal Reserve; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; or Commodity Futures Trading Commission) or a bank regulated by a state bank regulator;
- a department or agency of the United States, of any State, or of any political subdivision of any State;
- any entity established under the laws of the United States, of any State, or of any political subdivision of a State that exercises governmental authority on behalf of the United States, any State, or any political subdivision of a State;
- any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the Nasdaq Stock Market (except stock or interests listed under the separate “NASDAQ Capital Markets Companies” heading), provided that, if the person is a financial institution, other than a bank, only to the extent of its domestic operations; or
- a person that has an existing account with the broker-dealer, provided the broker-dealer has a reasonable belief that it knows the true identity of the person.

Accordingly, a broker-dealer is not required to verify the identities of persons with existing accounts at the firm, as long as the broker-dealer has a reasonable belief that it knows the true identity of the customer.

For purposes of the CIP rule, an “account” is defined as a formal relationship with a broker-dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loan and borrowing activity, and the holding of securities or other assets for safekeeping or as collateral. The following are excluded from the definition of “account”: (1) an account that the broker-dealer acquires through any acquisition, merger, purchase of assets or assumption of liabilities and (2) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA).

Rule: 31 C.F.R. § 1023.220.

Resources: [SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule \(October 1, 2003\)](#); [NTM 03-34](#); [FIN-2006-G007: Frequently Asked Question: Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative \(4/25/2006\)](#).

Describe how you will identify customers and verify their identities.

Note that a clearing firm does not have an obligation to perform CIP for an introduced customer if the clearing firm and the introducing firm have entered into a clearing agreement under which the functions of opening and approving customer accounts and directly receiving and accepting orders from the introduced customer are allocated

exclusively to the introducing firm and the functions of extending credit, safeguarding funds and securities, and issuing confirmations and statements are allocated to the clearing firm. This position also extends to piggybacking arrangements² where, pursuant to a piggybacking arrangement with an introducing firm, the piggybacking firm retains the functions of opening and approving customer accounts and directly receiving and accepting orders from introduced customers. Thus, under a piggybacking arrangement, the clearing firm and the introducing firm are not obligated to perform CIP for the customers introduced by the piggybacking firm, provided the proper agreement is in place.

Please note that a clearing firm's and introducing firm's AML programs should contain risk-based policies, procedures, and controls for assessing the money laundering risk posed by its fully disclosed clearing arrangements, for monitoring and mitigating that risk, and for detecting and reporting suspicious activity.

Resources: [FIN-2008-G002: Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations \(3/4/2008\)](#) and [FIN-2008-R008: Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution \(6/3/2008\)](#).

TEXT EXAMPLE:

EITHER:

In addition to the information we must collect under FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts), 17a-3(a)(17) (Customer Accounts) and Regulation Best Interest, we have 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.

OR:

² In a "piggybacking" arrangement, an introducing firm (the piggybacking firm) does not enter into a clearing agreement with a clearing firm, but rather establishes a relationship with an introducing firm that has established a clearing arrangement with a clearing firm, thus piggybacking off the introducing firm's clearing agreement. FIN-2008-G002 at p.2.

We do not open or maintain customer accounts within the meaning of 31 CFR 1023.100, in that we do not establish formal relationships with “customers” for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures. *(Note that a change in the firm’s business to accept customer accounts may be a material change in business requiring an application, review and approval by FINRA. See NASD Rule 1017).*

NOTE: *If your firm deals only with entities that are exempt from the definition of “customer,” describe how your firm will confirm and document that the entities are exempt.*

We will collect information to determine whether any entity opening an account would be excluded as a “customer,” pursuant to the exceptions outlined in 31 CFR 1023.100(d)(2)) (*e.g.*, documentation of a company’s listing information, licensing or registration of a financial institution in the U.S., and status or verification of the authenticity of a government agency or department).

Rule: 31 C.F.R. § 1023.220.

Resources: [SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule \(10/1/2003\)](#); [NTM 03-34](#).

a. Required Customer Information

Prior to opening an account, [*Name of person or category of associated person*] 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) the name;
- (2) date of birth (for an individual);
- (3) an address, which will be a residential or business street address (for an individual), 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), or a principal place of business, local office, or other physical location (for a person other than an individual); and
- (4) an identification number, which will be a taxpayer identification 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).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will [*add procedures describing who, what, when and how*] to confirm that the application was filed before the customer opens the account and to

obtain the taxpayer identification number within a reasonable period of time after the account is opened.

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.

Rule: 31 C.F.R. § 1023.220(a)(2)(i).

b. Customers Who Refuse to Provide Information

Describe your firm's policy for customers who do not provide requested 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, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR.

c. Verifying Information

Describe how you will verify customers' identities using the information described above. The information you gather may vary according to the risks posed by the type of account. The procedures must enable you to form a reasonable belief that you know the true identity of each customer. Among the risks to consider are the various types of accounts maintained by the firm, the various methods the firm uses to open accounts, the various types of identifying information available, and the firm's size, location and customer base. If you believe that some of these risk factors increase the likelihood that you will need more information to know the true identity of your customers, you should determine what additional identifying information might be necessary for a reasonable belief that you know the true identity of your customer and when such additional information should be obtained.

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. Christian Raburn 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).

We will verify customer identity through documentary means, non-documentary means or both. [*Tailor the sentence to your actual situation.*] We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We 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, we 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 a person other than an individual, documents 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.

We 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 [*identify reporting agency, database, etc.*];
- Checking references with other financial institutions; or
- Obtaining a financial statement.
- [*add other non-documentary methods, if applicable*]

We will use non-documentary methods of verification when:

- (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) 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.

We 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.

We recognize 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. We 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: *[Add additional procedures for verifying identity of certain customers, such as obtaining information about beneficial ownership, individuals with authority or control over such account. Remember to describe who will take the action, when and how they will obtain the information and what courses of action may be required.]*

Rule: 31 C.F.R. § 1023.220(a)(2)(ii).

d. Lack of Verification

Describe your procedures for responding to circumstances in which the firm cannot form a reasonable belief that it knows the true identity of a customer.

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.

Rule: 31 C.F.R. § 1023.220(a)(2)(iii).

e. Recordkeeping

Describe your recordkeeping procedures.

We 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.

Rule: 31 C.F.R. § 1023.220(a)(3).

f. Comparison with Government-Provided Lists of Terrorists

Describe how you will check government lists within a reasonable period of time after opening an account (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list). See [NTM 02-21](#), page 6. There currently are no government-provided lists of suspected terrorists that firms are required to use as part of their CIP.

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.

Rule: 31 C.F.R. § 1023.220(a)(4).

Resource: [NTM 02-21](#), page 6, n.24.

g. Notice to Customers

The CIP Rule requires you to provide adequate notice to customers that you are requesting information from them to verify their identities. You may provide such notice by a sign in your lobby, through other oral or written notice, or, for accounts opened online, notice posted on your website. No matter which methods of giving notice you choose, you must give it before an account is opened.

FINRA has produced a [Customer Identification Program Notice](#) to assist firms in fulfilling this notification requirement. Please refer to the [FINRA AML web page](#) for further details.

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: *[describe notice you will provide for each method of account-opening your firm uses (i.e., telephone, online, walk-in, etc.); the final rule provides the following sample language for notice to be provided to a firm's customers, if appropriate:]*

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

We 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 our 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.

[You will not be held responsible for the failure of the other financial institution to fulfill adequately your CIP responsibilities, provided that you can establish that your reliance was reasonable and you have obtained the requisite contracts and certifications.]

Rule: 31 C.F.R. § 1023.220(a)(6).

Resources: No-Action Letters to the Securities Industry and Financial Markets Association (SIFMA) ([February 12, 2004](#); [February 10, 2005](#); [July 11, 2006](#); [January 10, 2008](#); [January 11, 2010](#); [January 11, 2011](#); [January 9, 2015](#); [December 12, 2016](#); and [December 12, 2018](#))). (The letters provide staff guidance regarding the extent to

which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule.)

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, including broker-dealers. The Rule becomes 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, member firms 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 identify its ultimate beneficial owner(s) and not “nominees” or “straw men.”

The CDD Rule does not prescribe the form in which member firms 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 member firms obtain 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 applies 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. In addition to complying with existing SEC and FINRA record retention requirements, member firms must maintain the records collected for identification purposes for a minimum of five years after the account is closed, and for verification purposes, for five years after the record is made.

Member firms 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); FINRA Rule 3310.

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.](#)

TEXT EXAMPLE:

EITHER:

In addition to the information collected under the written Customer Identification Program, FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts), 17a-3(a)(17) (Customer Accounts) and Regulation Best Interest, we have 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.³ 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.

OR:

We do not open or maintain accounts for legal entity customers within the meaning of 31 CFR 1010.230. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures. *(Note that a change in the firm's business to accept accounts for legal entity customers may be a material change in business requiring an application, review and approval by FINRA. See NASD Rule 1017).*

NOTE: *If your firm deals only with entities that are exempt from the definition of "legal entity customer," describe how your firm will confirm and document that the entities are exempt or excluded.*

a. Identification and Verification of Beneficial Owners

TEXT EXAMPLE

At the time of opening an account for a legal entity customer, [*Name of person or category of associated person*] 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:

³ Beneficial owners and legal entity customers as defined by the CDD Rule.

- (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).

If your firm elects to utilize Appendix A to 31 CFR § 1010.230, record how the firm will use the document.

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 \(7/19/2016\)](#); [Regulatory Notice 17-40](#).

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.

TEXT EXAMPLE

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods [*describe*].

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); FINRA Rule 3310.

Resources: [FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions \(7/19/2016\)](#); [Regulatory Notice 17-40](#); [Regulatory Notice 18-19](#).

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 member firm detects information that is relevant to assessing the customer's risk profile, the member 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 member firm update customer information, including beneficial ownership information, on an ongoing or continuous basis.

TEXT EXAMPLE

We 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).

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(ii); FINRA Rule 3310.

Resources: [FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions \(7/19/2016\)](#); [Regulatory Notice 17-40](#); [Regulatory Notice 18-19](#).

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

Broker-dealers are prohibited from establishing, maintaining, administering or managing correspondent accounts in the United States for foreign shell banks. Broker-dealers also must take reasonable steps to ensure that any correspondent account established, maintained, administered or managed by the broker-dealer in the United States for a foreign bank is not being used by that foreign bank to indirectly provide banking services to a foreign shell bank. The BSA regulations allow covered financial institutions to receive a safe harbor for compliance with these requirements if they use the certification process described in the regulations. A covered financial institution must obtain a certification from each foreign bank for which it maintains a correspondent account “at least once every three years” to maintain the safe harbor.

In the context above, “correspondent account” is an account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank.

Foreign shell banks are foreign banks without a physical presence in any country. A “foreign bank” is any bank organized under foreign law or an agency, branch or office of a bank located outside the U.S. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

The prohibition does not include foreign shell banks that are regulated affiliates. Foreign shell banks that are regulated affiliates are affiliates of a depository institution, credit union or foreign bank that maintains a physical presence in the U.S., or a foreign country, and are subject to supervision by a banking authority in the country regulating that affiliated depository institution, credit union or foreign bank. Foreign branches of a U.S. broker-dealer are not subject to this requirement, and “correspondent accounts” of

foreign banks that are clearly established, maintained, administered or managed only at foreign branches are not subject to this regulation.

Describe how your firm will identify foreign banks with which the firm has accounts, and then detect and close correspondent accounts for foreign shell banks.

NOTE: *If your firm does not establish, maintain, administer or manage correspondent accounts for foreign banks, state that this is your firm's policy and describe the internal controls that your firm will implement to detect any attempt to open a correspondent account.*

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks by [*describe procedure to detect such accounts*]. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

Rule: 31 C.F.R. § 1010.630; 31 C.F.R. § 1010.605.

b. Certifications

Describe your process for obtaining certain required information from any foreign bank account holders and for obtaining the necessary certifications at least once every three years to rely on the safe harbor provided by the BSA regulations.

We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

Rule: 31 C.F.R. § 1010.630(b).

Resources: [FinCEN's Chapter X web page](#); [Certification Regarding Correspondent Accounts for Foreign Banks](#); [Recertification Regarding Correspondent Accounts for](#)

[Foreign Banks; FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 \(2/3/2006\).](#)

c. Recordkeeping for Correspondent Accounts for Foreign Banks

Firms must keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

Rule: 31 C.F.R. § 1010.630(e).

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

The Secretary of the Treasury or the Attorney General of the United States may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and may request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank. The summons or subpoena may be served on the foreign bank in the United States if the foreign bank has a representative in the United States, or in a foreign country pursuant to any mutual legal assistance treaty, multilateral agreement or other request for international law enforcement assistance.

A broker-dealer that maintains a correspondent account for a foreign bank in the United States must maintain records in the United States identifying the owners of such foreign bank whose shares are not publicly traded and the name and street address of a person who resides in the United States and is authorized, and has agreed to be an agent to accept service of legal process for the foreign bank's correspondent account. Upon receipt of a written request from a federal law enforcement officer for this information, the broker-dealer must provide such information to the requesting officer no later than seven days after receipt of the request.

Additionally, such broker-dealer must terminate any correspondent relationship with a foreign bank not later than 10 business days after receipt of written notice from the Secretary of the Treasury or the Attorney General of the United States that the foreign bank has failed to: (1) comply with a summons or subpoena issued by these two entities; or (2) initiate proceedings in a United States court contesting such summons or subpoena.

Describe your firm's procedures for handling requests from federal law enforcement officers for the information described above, and if necessary, terminating a correspondent relationship with a foreign bank that has failed to comply or contest a

summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States.

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these correspondent accounts.

Rule: 31 C.F.R. § 1010.670.

8. 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.

A foreign financial institution is:

- (1) a foreign bank;*
- (2) any branch or office located outside the United States of a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company;*
- (3) any other person organized under foreign law (other than a branch or office of such person in the United States) that, if it were located in the United States, would be a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company; and*
- (4) 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.*

A person, 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. “Account” is defined as any formal relationship established with a broker or dealer in securities to provide regular services to effect transactions in securities, including but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral.

For broker-dealers, correspondent accounts established on behalf of foreign financial institutions include, but are not limited to: (1) accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase programs; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivative contracts.

On January 30, 2008, FinCEN issued guidance clarifying that covered financial institutions (which includes U.S. broker-dealers) 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 \(1/30/2008\)](#).

Describe your firm’s due diligence program for any correspondent accounts established on behalf of foreign financial institutions.

We 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.

We 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. *[Describe in detail all of the firm’s procedures for periodically reviewing foreign financial institution account activity].*

OR:

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions *[and describe the internal controls that your firm will implement to detect any attempt to open one of these types of accounts].*

Rule: 31 C.F.R. § 1010.610(a).

Resource: [FIN-2006-G009: Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries \(5/10/2006\).](#)

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 subaccount, 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 securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

Rule: 31 C.F.R. § 1010.610(b); 31 C.F.R. § 1010.610(c).

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

A firm must include procedures to follow in circumstances where the firm 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 Private Banking Accounts/Senior Foreign Political Figures

Describe your firm's due diligence program for "private banking" accounts for non-U.S. persons. Firms must have a due diligence program that is reasonably designed to detect and report any known or suspected money laundering conducted through or involving any private banking account maintained by or on behalf of a non-U.S. person, as well as the existence of the proceeds of foreign corruption in any such account. This requirement applies to all private banking accounts for non-U.S. persons, regardless of when they were opened. Accounts requested or maintained by or on behalf of "senior foreign political figures," which is defined below and includes their immediate family members and close known associates, require enhanced scrutiny.

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of \$1,000,000, is established for one or more individuals and is assigned to or administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

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.

NOTE: If your firm does not open or maintain private banking accounts, state that this is your firm's policy.

TEXT EXAMPLE:

EITHER:

We will review our accounts to determine whether we offer any private banking accounts and we will conduct due diligence on such accounts. This due diligence will include, at least: (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior

foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then we may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification. If a higher risk is apparent, we will consider additional due diligence measures such as [*describe in detail the additional measures*].

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, we will, after consultation with the firm's AML Compliance Person and, as appropriate, not open the account, suspend the transaction activity, file a SAR, close the account and/or take other appropriate action.

OR:

We do 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

Describe how your 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, such as broker-dealers, 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](#).

EITHER:

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, 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, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

OR:

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, we understand 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, we will take the following steps:

- (1) We will review our account records, including correspondent account records, to ensure that our accountholders and correspondent accountholders 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 Accountholders

We will notify our correspondent accountholders that the account may not be used to provide the Specified Banks with access to us [*provide details of what the language of the notice will state*].

We will transmit the notice to our correspondent accounts using the following method [*specify*], 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 accountholders 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); [NTM 07-17](#); [NTM 06-41](#).

11. Monitoring Accounts for Suspicious Activity

Broker-dealers must establish risk-based procedures reasonably designed to detect and report suspicious transactions in order to comply with the BSA and FINRA Rule 3310. 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. Your 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 your firm's monitoring procedures be tailored to your 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.

Your procedures should also describe how the firm will monitor for or otherwise identify these “red flags.” Your 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 and include, among other things, securities fraud.

It is important that your procedures provide specific details regarding your firm’s monitoring system (e.g., who, what, when, where and how).

We 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 the following methods: *[describe]*. *[If automated monitoring is utilized, your procedures should include a list of reports as well as their purpose and description. If manual monitoring is utilized, your procedures should include a list of documents/systems to be reviewed and the purpose of the review. Regardless of the method, your procedures should 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 *[Add if appropriate: in consultation with {Name or title} OR with the approval of {Name or title}]* 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.

We will conduct the following reviews of activity that our monitoring system detects: *[describe]*. We will document our monitoring and reviews as follows: *[describe]*. The AML Compliance Person 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. Relevant information can include, but not be limited to, the following: *[describe]*.

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.

Resource: [67 Fed. Reg. 44048 \(July 1, 2002\) \(Final Rule: Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions\)](#) it is intended that broker-dealers, and indeed every type of financial institution to which the suspicious transaction reporting rules of 31 CFR part 103 apply, will evaluate customer activity and relationships for money laundering risks, and design a suspicious transaction monitoring program that is appropriate for the particular broker-dealer in light of such risks”).

a. Emergency Notification to Law Enforcement by Telephone

Describe when and how your firm will call the appropriate law enforcement authority in emergencies.

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 (*insert contact number*), local FBI office (*insert contact number*) and local SEC office (*insert contact number*) (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely a SAR.

Although we are not required to, in cases where we have filed a SAR that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR or notify an appropriate law enforcement authority.

Rule: 31 C.F.R. § 1023.320.

Resources: [FinCEN's website](#); [OFAC web page](#); [NTM 02-21](#); [NTM 02-47](#).

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 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 company¹⁰ 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 for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
- An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
- An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, 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 Deposits of Securities

- A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
- A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
- A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
 - were recently issued or represent a large percentage of the float for the security;
 - reference a company or customer name that has been changed or that does not match the name on the account;
 - were issued by a shell company;
 - were issued by a company that has no apparent business, revenues or products;
 - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
 - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
 - were issued by a company that has been the subject of a prior trading suspension; or
 - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.
- The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.
- A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.
- The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.
- The customer deposits physical securities or delivers in shares electronically, and within a short timeframe, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
- Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

Potential Red Flags in Securities Trading

- The customer, for no apparent reason or in conjunction with other “red flags,” engages in transactions involving certain types of securities, such as penny stocks, Regulation “S” stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer’s activity.)
- There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
- The customer’s activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.
- A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.
- Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.
- A customer accumulates stock in small increments throughout the trading day to increase price.
- A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.
- A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.
- A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.
- A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of “spoofing”).
- A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of “layering”).
- Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.
- The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.
- The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry but does so at an opportune time) and there is no reasonable explanation for the change.
- The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.
- The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.
- The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depositary Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.
- The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.
- The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

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 securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, 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 nostro¹⁴ 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.
- A person customarily uses the ATM to make several deposits into a brokerage account 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.

Potential Red Flags in Insurance Products

- The customer cancels an insurance contract and directs that the funds be sent to a third party.
- The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.
- The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied by suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.
- The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- The customer purchases an insurance product with no concern for the investment objective or performance.

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.
- Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
- Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
- 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.
- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
- The customer does not exhibit a concern with the cost of the transaction or fees (e.g., surrender fees, or higher than necessary commissions).
- A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
- There is an unusual use of trust funds in business transactions or other financial activity.

Resource: [Regulatory Notice 19-18](#)

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 [*include procedures 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

Describe your firm's procedures for identifying any suspicious transactions and determining if they need further investigation or warrant filing a SAR. These procedures should also cover the maintenance of SAR documentation and the preservation of its confidentiality, and BSA reporting. Note that firms must exercise due diligence in monitoring suspicious activity as the regulations require firms to file a SAR when they "know, suspect, or have reason to suspect" that transactions involve certain suspicious activities.

Firms are exempt 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; (2) lost, missing, counterfeit or stolen securities that the firm has reported pursuant to Exchange Act Rule 17f-1; and (3) violations of the Federal securities laws or self-regulatory organization (SRO) rules by the firm, its officers,

directors, employees or registered representatives, that are reported appropriately to the SEC or SRO, except for a violation of Exchange Act Rule 17a-8, which must be reported on a SAR. However, if a firm relies on one of these exemptions, it may be required to demonstrate that it relied on one of these exemptions and must maintain records, for at least five years, of its 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

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our 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.

We 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. In addition, although we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. *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.

We 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.

We 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.

We 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 securities regulators or SROs upon request.

We 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, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, 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; FINRA Rule 3310.

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 instrument is being used in an attempt to avoid the reporting of the transaction.”

[Include this language if your firm prohibits transactions involving currency] Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions: *[Describe]*. 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. A CMIR is not required to be filed by a securities broker-dealer 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.

[Include this language if your firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to the firm 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:] Our 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 broker-dealers to report and keep records related to any financial interest in, or signature authority over, a bank account, securities account or other financial account that the firm has in a foreign country in which the aggregate value of any accounts exceed \$10,000.

We 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.

TEXT EXAMPLE:

EITHER:

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.

OR:

When we issue or sell a bank check or draft, cashier's check, money order or traveler's check in the amounts of \$3,000 to \$10,000 inclusive, we will maintain records of the following information:

- (a) (1) If the purchaser has a deposit account with us:

- (i)
 - (A) the name of the purchaser;
 - (B) the date of purchase;
 - (C) the type(s) of instrument(s) purchased;
 - (D) the serial number(s) of each of the instrument(s) purchased; and
 - (E) the amount in dollars of each of the instrument(s) purchased.
 - (ii) In addition, we must verify that the individual is a deposit accountholder or must verify the individual's identity. Verification may be either through a signature card or other file or record provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record; or by examination of a document which is normally acceptable as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, we shall verify the deposit accountholder's identity by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser, and shall record the specific identifying information (*e.g.*, driver's license number and state of issuance).
- (2) If the purchaser does not have a deposit account with us:
- (i)
 - (A) the name and address of the purchaser;
 - (B) the Social Security number of the purchaser, or if the purchaser is an alien and does not have a Social Security number, the alien identification number;
 - (C) the date of birth of the purchaser;
 - (D) the date of purchase;
 - (E) the type(s) of instrument(s) purchased;
 - (F) the serial number(s) of the instrument(s) purchased; and

- (G) the amount in dollars of each of the instrument(s) purchased.
- (ii) In addition, we shall verify the purchaser's name and address by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser, and shall record the specific identifying information (e.g., driver's license number and state of issuance).
- (b) Contemporaneous purchases of the same or different types of instruments totaling \$3,000 or more shall be treated as one purchase. Multiple purchases during one business day totaling \$3,000 or more shall be treated as one purchase if an individual employee, director, officer or partner of the [Name of Firm] has knowledge that these purchases have occurred.
- (c) We shall keep records required to be kept for a period of five years, and such records shall be made available to the federal and state authorities or SROs upon request at any time.

Rule: 31 C.F.R. § 1010.415.

Resource: 59 Fed. Reg. 52250 (October 17, 1994) (Final Rule; Amendments to BSA Regulations Relating to Identification Required to Purchase Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks).

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.

Rules: 31 C.F.R. § 1010.410(e) and (f); Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

13. AML Recordkeeping

a. Responsibility for Required AML Records and SAR Filing

Your firm must establish procedures to maintain all applicable AML program records and reviews.

Our AML Compliance Person 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, our 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, including certain SEC rules that require six-year retention periods (e.g., Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

Rules: 31 C.F.R. § 1010.430; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

b. SAR Maintenance and Confidentiality

Describe your firm's retention and confidentiality requirements for SARs.

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR. 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. [*Describe any other retention or confidentiality procedures of your firm 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.

Rule: 31 C.F.R. § 1023.320(e).

Resources: 67 Fed. Reg. 44048 (July 1, 2002) (Final Rule; Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions); [NTM 02-47](#).

c. Additional Records

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

TEXT: We shall retain either the original or a microfilm or other copy or reproduction of each of the following:

- 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, investment securities or credit, of more than \$10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) 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, investment securities or credit, 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;
- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);
- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than \$10,000 to a person, account or place, outside the U.S.; and
- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, 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.

Rules: 31 C.F.R. § 1010.410; 31 C.F.R. 1023.410; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

14. Clearing/Introducing Firm Relationships

Describe how you and your clearing firm will comply with your independent AML obligations, which include describing the exception reports, if any, you obtain from your clearing firm, how frequently the reports will be reviewed and by whom, what review or inquiry will be conducted regarding exceptions, and how that review will be evidenced.

We will work closely with our clearing firm 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 our firm and our clearing firm have filed (and kept updated) 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*] and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm 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.

*Rules: 31 CFR § 1010.540; FINRA Rule 3310; FINRA Rule 4311.
Resource: [NTM 02-21](#).*

15. Training Programs

Describe your AML ongoing employee training and programs.

We 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 our 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.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. Currently our training program is: [*insert specifics, such as "all registered representatives must view the video entitled "Spotting Money Laundering" by X date or within two weeks of being hired, etc.*] We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our 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); FINRA Rule 3310.
Resources: See [NTM 02-21](#), [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

Describe your firm's independent testing function to assess its AML compliance program. You must choose whether your firm's personnel or a qualified outside party will perform this function. Your decision will depend on your firm's size and resources. Independent testing is generally to be performed annually (on a calendar year basis). A firm that does not execute transactions for customers or otherwise hold customer accounts and does not act as an introducing broker with respect to customer accounts (e.g., engages solely in proprietary trading or conducts business only with other broker-dealers) may generally

perform an independent test every two calendar years. All firms should undertake more frequent testing than required if circumstances warrant.

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

a. Staffing

EITHER

The testing of our AML program will be performed at least annually (on a calendar year basis) *[or if a firm is eligible, the firm may state "every two calendar years"]* by ComplyAdvantage, an independent third party. 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. Christian Raburn also has the responsibility of keeping Integrity Trade's PCI Compliance current. Independent testing will be performed more frequently if circumstances warrant.

OR

The testing of our AML program will be performed at least annually (on a calendar year basis) *[or, if the firm is eligible, every two calendar years]* by *[Names]*, personnel of our firm, none of whom are *[who is not]* the AML Compliance Person nor do they *[he/she]* perform the AML functions being tested nor do they report to any such persons. Their *[his/her]* qualifications include a working knowledge of applicable requirements under the BSA and its implementing regulations *[and—describe any additional qualifications]*. To ensure that they *[he/she]* remain independent, we will separate their *[his/her]* functions from other AML activities by using a certified third-party. Independent testing will be performed more frequently if circumstances warrant.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.

Resource: [NTM 06-07](#).

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.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.

17. Monitoring Employee Conduct and Accounts

Describe how your firm will monitor employee accounts for potential signs of money laundering. Your firm must subject employee accounts to the same account identifying and monitoring procedures as customer accounts. Your firm should also review supervisors' performance of their AML responsibilities.

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 [*Christian Raburn – a member of senior management.*]

Rules: 31 C.F.R. § 1023.320; 31 C.F.R. § 1023.210; FINRA Rule 3310.

18. Confidential Reporting of AML Non-Compliance

Describe how you ensure that employees who report suspected violations of AML compliance are protected from retaliation.

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.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

19. Additional Risk Areas

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. The major additional areas of risk include UOB Proxies. Additional procedures to address these major risks are using AI tools provided by ComplyAdvantage software.

20. Senior Manager Approval

A firm's AML compliance program must be approved, in writing, by a member of senior management.

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

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

Signed: 

CHRISTIAN RABURN

Title: MBR, INTEGRITY TRADE LLC

Date: 02/06/2024