LUXOLO FINANCIAL

Policy for Compliance with Federal Anti-Money Laundering Regulations

“AML Policy”

Revised 12.27.2017

Contents

1. Introduction

LUXOLO, LLC (the "Company") is a financial services company, serving both consumers and businesses. The Company primarily provides digital currency exchange services both via automated teller machine(s) and via speaking or meeting directly with Company staff to conduct an exchange transaction.

1.1. Regulatory Authority

For federal and state regulatory purposes, the Company is classified as a Money Service Business and Money Transmitter.

As such, the Company is required to comply with requirements of the Bank Secrecy Act [31 USC 5311, pub. 1982, rev. 2001] (hereinafter, the "BSA") to help the government detect and combat money laundering and criminal activity financing. BSA laws are enforced by the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN"), with whom the Company is registered as #31000115857440.

The Company is not a broker-dealer and therefore is neither regulated by Financial Industry Regulatory Authority, Inc ("FINRA") nor the Securities and Exchanges Commission ("SEC") and will not report to either entity.

Accordingly, we have developed and structured an appropriate program of policies and procedures (the "AML Policy") in order to comply with BSA requirements.

2. Summary

To meet or exceed these regulatory requirements, the Company:

- Developed this AML Policy incorporating policies, procedures, internal controls and record keeping to reasonably designed to assure compliance with BSA;
- Designated a compliance officer at the Company responsible for day-to-day compliance with BSA by administering this AML Policy;
- Provides ongoing training to appropriate Company personnel regarding their responsibilities under this AML Policy;
- Provides a formal annual review of this AML Policy and makes revisions and adjustments as necessary.

3. AML Policy

It is the policy of LUXOLO, LLC to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of criminal and terrorist activities. We will comply with all applicable requirements and regulations.

3.1. Background

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: (i) 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 travelers checks, or deposited into accounts at financial institutions; (ii) in 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; (iii) 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.

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 organisations. 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 regulations and will be reviewed and updated at least annually 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. § 103.120(c); FINRA Rule 3310.

3.2. AML Compliance Person and Duties

The firm has designated Daren Hebold as its Anti-Money Laundering Program Compliance Person (“AML Compliance Person”), with full responsibility for the firm’s AML Policy. Mr. Hebold has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, outlined on his professional resume which is attached to this document as an Exhibit.

The duties of the AML Compliance Person will include monitoring the firm’s compliance with AML obligations, and overseeing communication and training for employees. 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 (“SAR-SFs”) are filed with FinCEN when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm’s AML program.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310, NASD Rule 1160.

Resources: NTM 06-07; NTM 02-78. If applicable, firms can submit their AML Compliance Person information through FINRA's FCS Web page.

4. Granting AML Information to Federal Law Enforcement Agencies

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

We will respond to a 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 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. Our AML Compliance Person or designee(s) will 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, our AML Compliance Person 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), we will structure our search accordingly. If our AML Compliance Person searches our records and does not find a matching account or transaction, then we will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by either i) 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 ii) 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. Our AML Compliance Person 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. § 103.100.

Resources: FinCEN press release (2/6/03); FinCEN press release (2/12/03); NASD Member Alert (2/14/03); FinCEN's 314(a) Fact Sheet (11/18/08). 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 at (800) 949-2732.

4.2. National Security Letters

National Security Letters ("NSLs") are written investigative demands that may be issued by the local Federal Bureau of Investigation 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-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

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

4.3. Grand Jury Subpoenas

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-SF). 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-SF in accordance with the SAR-SF 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 in confidence. If we file a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF 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).

4.4. 4.4. Information Sharing With Other Financial Institutions

Under USA PATRIOT Act Section 314(b), financial institutions may voluntarily share information in satisfying BSA regulations.

It is not the Company's policy to share customer information with other financial institutions. However, in the event the Company receives credible information from another financial institution about a suspicious customer who may have conducted or may intend to conduct business with the

Company, the AML Compliance Person will document such information and considering the risks involved, decide what appropriate action(s) to take, if any.

Rule: 31 C.F.R. § 103.110.

5. Customer Identification Program

5.1. General Provisions

The Company has established, documented and maintains a Customer Identification Program ("CIP"). It is the Company's policy to collect certain minimum customer identification information from each customer that is tiered based on daily transaction volume; 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.

5.2. Tiers of Required Customer Information

For customers meeting all of the Company's above criteria, it is the Company's policy to collect customer identification information commensurate with tiered daily transaction volume limits.

- Tier I Transactions: Customers who wish to conduct a transaction or transactions with the Company totaling up to Seven Thousand Five Hundred Dollars (USD $7,500) per day will be required to submit the following customer identification information:
    - a domestic cellular telephone number including area code;
    - a "yes" or "no" response to a question asking the customer to acknowledge they are conducting this transaction on their own behalf, have obtained the deposit funds lawfully and do not intend to fund terrorism.

- Tier II Transactions: Customers who wish to conduct a transaction or transactions with the Company totaling an amount between Seven Thousand Five Hundred One Dollars (USD $7,501) and One Hundred Thousand (USD $100,000) per day will be required to submit the following customer identification information:
    - Full name;
    - Date and place of birth;
    - Physical address (individual) or place of business (corporate);
    - Federal Tax ID number (individual or corporate);
    - Email address;
    - Domestic telephone number with area code;
    - "Basic" Customer Due Diligence information defined below.

- Tier III Transactions: Customers who wish to conduct a transactions or transactions with the Company in the amount of One Hundred One Thousand One (USD $100,001) per day or higher

will be required to submit all of the above customer identification information, together with "Enhanced" Customer Due Diligence information defined below.

5.3. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The AML Compliance Person or designee 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).

Documentary Methods
We will verify customer identity through documentary means, non-documentary means or both. 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, 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.

Non-Documentary Methods
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.];
- Obtaining a financial statement containing identity information about the customer.

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 prior to conducting a transaction with the customer. 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-SF 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.

Rule: 31 C.F.R. §103.122(a)(1)(i)(ii) and 103.122(a)(4)(i)(ii) and 31 C.F.R. §103.122(b)
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification
Program Rule (October 1, 2003); NTM 03-34; FIN-2006- G007: Frequently Asked

5.4. Refusal to Provide Customer 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, or otherwise offers responses containing "Red Flags" described below, then our firm will decline business service offerings to that customer. Additionally, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR-SF.

5.5. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not conduct a transaction; (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 customer's identity fail; and (4) determine whether it is necessary to file a SAR-SF in accordance with applicable laws and regulations.

Rule: 31 C.F.R. §103.122(b)(2)(iii).

5.6. Customer Criteria

It is the Company's policy to only conduct transactions with customers who meet all of the following minimum criteria:

5.6.a. Domestic Customers

- US Citizen with domestic residence or place of business, as applicable;
- Source of funds must be either cash, or electronic funds from a domestic banking institution (foreign bank funds not accepted), or cryptocurrency held either personally or on a domestic exchange;
- Customer must not be on any government-provided lists of suspected terrorists.

5.6.b. Foreign Customers

It is not the policy of this Company to conduct business with foreign customers.

If the customer does not meet all of the above criteria and/or we cannot reasonably confirm this information, the Company at its sole discretion via its AML Compliance person or designee, will decline to offer services to that customer.

5.7. Record Keeping

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 last transaction has been processed; 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. §103.122(b)(3).

5.8. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after their most recent transaction (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. §103.122(b)(4).
Resources: NTM 02-21, page 6, n.24; 31 C.F.R. § 103.122.

5.9. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities and certain other qualifying information as required by federal law. We will post this notice on our website, lobby and transaction related materials in order that prospective customers can review this information prior to engaging in a transaction with the Company.

Rule: 31 C.F.R. §103.122(b)(5).

5.10. Customer Due Diligence

It is important to our AML and SAR-SF reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. Prior to conducting a transaction for a customer, the Customer Due Diligence ("CDD") we may perform will be in addition to customer information obtained for purposes of our CIP.

Where we believe that additional customer due diligence is warranted, we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. In considering the apparent and/or perceived risks of providing services to a prospective customer, the Company in its sole discretion reserves its right to decline to offer services to customers who do not meet these criteria and/or are deemed pose high risk under the provisions of this Policy.

5.10.a. Basic Customer Due Diligence information

For Tier I Transactions defined above, Customer Due Diligence information is not required. For Tier II Transactions define above, Customer Due Diligence is required and the Company at the discretion of the AML Compliance Person may require some or all of the following:

- the source of the customer's funds;
- the intended destination of exchanged funds.

5.10.b. Enhanced Customer Due Diligence Information

For Tier III Transactions defined above, Customer Due Diligence information is required and must include all of the following:

- the source of the customer's funds;
- the intended destination of exchanged funds;
- the customer's occupation and business;
- the beneficial owners of the business;

- banking reference(s).

The above Customer Due Diligence information shall be obtained by the Company via a questionnaire taken either in-person or over the telephone. This information shall be considered a company record subject to record keeping requirements contained herein.

We will also ensure that the customer information remains accurate by asking customers to update their information with us prior to each subsequent transaction.

6. Suspicious Transactions and BSA Reporting

6.1. Red Flags for Suspicious Activity

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

Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.
- Customer with no discernable reason for requesting the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- "Structures" exchanges, transactions or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.
- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
- Customer's explanation of how he or she acquired the certificate does not make sense or changes.
- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.
- Law enforcement subpoenas.
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to customer.
- No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).

6.2. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the AML Compliance person or designee. Under the direction of that person, the Company will determine the severity and urgency of the matter, if any. We will decide whether or not and how to further investigate the matter, assess the risks and determine the course of action.

The course of action may include taking no action, gathering additional information internally or from third-party sources, contacting the government, freezing a transaction and/or filing an SAR-SF.

6.2.a. Emergency Notification to Law Enforcement

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 SAR-SF.

Rule: 31 C.F.R. § 103.19.
Resources: FinCEN's Web site; OFAC Web page; NTM 02-21; NTM 02-47.

6.3. BSA Reporting

6.3.a. Filing an SAR-SF

We will file SAR-SFs 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-SF and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. 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-SF reporting the violation.

We may file a voluntary SAR-SF 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 SAR-SFs 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-SF.

We will report suspicious transactions by completing a SAR-SF, 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-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF 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-SF 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-SF or the information contained in the SAR-SF will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

Rules: 31 C.F.R. §103.19, FINRA Rule 3310(a).
Resources: FinCEN's website contains additional information, including information on the BSA E-Filing System, the SAR-SF Form (fill-in version), and the biannual SAR Activity Reviews and SAR Bulletins, which discuss trends in suspicious reporting and give helpful tips. SAR Activity Review, Issue 10 (May 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.

6.3.b. Currency Transaction Reports

We are required to 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 paper money of the United States or of any other country" that is "customarily used and accepted as a medium of exchange in the country of issuance." Currency includes U.S. silver certificates, U.S. notes, Federal Reserve notes, and official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.

If we discover such transaction(s) has/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 CTR Form provided on FinCEN's website.

Rules: 31 C.F.R.§§103.11, 103.22.
Resource: BSA E-Filing System.

6.3.c. Monetary Instrument Purchases

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.

Rule: 31 C.F.R. § 103.29. See also 31 C.F.R. 103.22(b).

7. AML Recordkeeping

7.1. Responsibility for Filing Required AML Records and SAR-SF Reports

Our AML Compliance Person and designee will be responsible for ensuring that AML records are maintained properly and that SAR-SFs are filed as required. In addition, as part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (See Section 5 above) and funds transmittals.

We will maintain SAR-SFs and their accompanying documentation for at least five years.

Rules: 31 C.F.R. § 103.38, 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.

7.2. SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs 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-SF. We will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive.

We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Person will handle all subpoenas or other requests for SAR-SFs.

Rules: 31 C.F.R. §103.19(e); 67 Fed. Reg. 44048, 44054 (July 1, 2002).
Resources: NTM 02-47.

7.3. Additional Records

We shall retain either the original, a photocopy or digital copy of each of the following:

- 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. §§ 103.33, 103.35(b).

7.4. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person. 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 SAR-SFs);
(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.

Rule: FINRA Rule 3310.
Resources: See NTM 02-21, FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007).

7.5. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm’s AML compliance program to the AML Compliance Person. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

7.6. Senior Management Approval

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. § 103.120; FINRA Rule 3310.

Signed: _____ Printed: _____

Title: _____

Date: _____

8. Exhibits

8.1. Professional Resumes

8.1.a. Daren Hebold, AML Compliance Person

8.1.d. Arnold Jackson, AML Compliance Person designee (for select duties)