MONEYTUN LLC
3651 LINDELL RD. STE D-225
LAS VEGAS, NV 89103

MONEYTUN LLC

COMPLIANCE MANUAL

AML POLICIES & PROCEDURES

(Updated 02/10/2014)

Table of Contents

Compliance Program

This Compliance Manual, Policies and Procedures were reviewed and approved for publication and distribution to its employees by MONEYTUN's sole owner.

MONEYTUN is a sole owner LLC. It does not have Board of Directors, however, Arthur Avetisian is the Compliance Officer.

The Bank Secrecy Act ("BSA") as amended by the USA Patriot Act classifies MONEYTUN LLC. ("MONEYTUN") and its Agents as Money Services Business ("MSB"). MSBs are non-banking financial institutions that provide financial products and services. The regulations classify "check cashers," "money order issuers," "money transmitters," "currency exchanges," "traveler check issuers," and "stored value card issuers" as Money Services Businesses. MONEYTUN has to develop a compliance program that must be risk based. MONEYTUN is required to identify, assess, and mitigate the risks that its business will be abused by criminals for money laundering and terrorist financing. Risks can be jurisdictional, product-related, service-related, Agent-related, Paying-Agent-related, Employee-related, service-related or Customer-related.

Regardless of where these risks arise, MONEYTUN must take reasonable steps to mitigate them. Compliance is risk-based, meaning that MONEYTUN must devote more compliance resources to the areas of its business that pose the greater risks.

MONEYTUN expects an effective implementation of its compliance program. The expectation is predicated upon each MONEYTUN Employee's and each MONEYTUN Agent's knowledge of the business, understanding of the applicable laws and regulations and a careful assessment of vulnerability to money laundering and terrorist financing.

Compliance Policy

MONEYTUN actively participates in domestic and international efforts to combat money laundering, terrorist funding and other financial crimes. MONEYTUN complies with all applicable laws and regulations relating to such activities, and seeks all available means to prevent being utilized as a conduit for such illicit funds.

Compliance Standards

MONEYTUN expects all of its Employees and Agent to observe the following Compliance standards:

- Always conduct business in accordance with the highest ethical standards.
- Follow MONEYTUN's "Know Your Customer" program included in this Manual.
- Always be alert to Customer transactions that may indicate money laundering or other criminal activity; and take proper steps to report and/or refuse such transactions.
- Cooperate with law enforcement authorities within the confines of applicable law, and report any suspicious activities to the MONEYTUN's Compliance Officer.
- Fully comply with the recordkeeping and reporting requirements of the BSA and its regulations.
- Maintain all records required by the BSA, the USA Patriot Act and all applicable anti-money laundering laws and regulations, for the required specified time period, at a minimum.
- Comply with all applicable Federal, State regulations and local laws.
- Refuse to conduct Money Transfer transactions if a Customer fails to provide sufficient identification or other required information. Depending on the circumstances may file SAR as a result.
- File suspicious activity reports on transactions that involve or aggregate up to $2,000 or more and MONEYTUN knows, suspects or has reason to suspect that the transaction is being with the intent to evade the record keeping or reporting requirements, or that the funds have been originated from an illegal activity.

Review transactions daily for possible structuring to evade reporting requirements.

Four Pillars of Compliance

MONEYTUN compliance program consists of the following four areas:

1. Approved internal policies, procedures and controls for:
   Detecting structured transactions or transactions conducted in a way to prevent the record-keeping or documentation requirements of the BSA or OFAC. MONEYTUN's computerized compliance monitor reviews each transaction to ensure the transaction is properly documented and/or reported as required. All transactions, regardless of amount, are filtered against a current data base based on preprogrammed compliance rules, including OFAC. Any transaction, regardless of the amount, that matches any of the predefined rules is automatically placed on hold for further review by a transaction analyst. Once a transaction is placed on hold it will not be released until the transaction is properly documented as defined in the Compliance Manual's Procedures Section.

- Detecting attempts to utilize MONEYTUN as a conduit for illicit funds;
- Preventing money laundering or terrorist financing;
- Know Your Customer, Employee, Agent, Paying Agent and Customer Procedures. MONEYTUN's Compliance Program incorporates Know Your Customer guidelines issued by FinCEN and other applicable regulatory authorities, the program also provides comprehensive training to its Employees and Agents on a regular basis. In furtherance of the KYC obligations, MONEYTUN has established due diligence procedures to ensure that the identity of its Customers and Agents is known
- reviewing customer identification;
- Creating and retaining transaction records;
- Responding to law enforcement requests.
- Reporting suspicious transactions; and
- Reporting large currency transactions.
- Mystery Shopping. The purpose of the mystery shopping program is to detect and mitigate risks by implementing targeted training to employees and agents. (This program will be implemented whenever Moneytun's agent and branch network reaches 5 or more locations)
- In order to comply with its responsibilities under the Bank Secrecy Act, the USA Patriot Act, OFAC and all other applicable federal and state laws and regulations, MONEYTUN has created a Compliance Department headed by its Compliance Officer. The Compliance Department is organized in four basic functions: Regulatory, Transaction Analysis and Reporting, Training, and Agent Management.

2. MONEYTUN has designated Arthur Avetisian as its Compliance Officer. The Compliance Officer is responsible for the Compliance Program. The Compliance Officer's responsibilities include the following::
    - Ensuring that all compliance Policies and Procedures are followed;
    - Proposing new compliance policies and procedures
    - Procedures are updated as needed to meet all federal, state, local laws and regulations.
    - Provides training to all compliance personnel to ensure proper application of all policies and procedures and identification of risks and attempts to utilize MONEYTUN by unscrupulous criminals to launder money or finance terrorism and compliance with all applicable laws and regulations.
    - Training and education are provided to all Employees, Agent and Paying Agents
    - Implementing a record retention program
    - Develop policies and procedures for the protection of the customers' information
    - Develop and implement an agent management and oversight program that includes agent visitation to audit agent's compliance with applicable policies and procedures, laws and regulations.
    - Work closely with MONEYTUN's agent to help them develop their own compliance program as required by the laws and regulations.

3. An ongoing Agent and Employee training program that:
    - Explains policies and procedures;
    - Explains the applicable laws and regulations;
    - Provides updates to maintain Employees and Agent current with their responsibilities and obligations under the applicable laws and regulations;
    - Provides guidance in identifying suspicious activity or transactions that are conducted with the intention to prevent the record-keeping or reporting requirements of the applicable laws and regulations;.
    - Teaches the record-keeping and reporting obligations of the Employees and Agents under the applicable laws and regulations.

4. An independent review of the Anti Money Laundering ("AML") program:
    - MONEYTUN will have external examinations of its compliance program by MONEYTUN's Internal Audit Department (when the function is formally established) and an independent external AML expert;

- MONEYTUN's Internal Audit Department will conduct frequent reviews of the compliance program. The reviews will include, branches and agents visitation to review Agent's and Employees' knowledge of the Policies and Procedures, the BSA and all other applicable laws and regulations, record-keeping and mystery shopping The independent examination external examination;
- The external examination by the AML expert will focus on the compliance program and its application. The external expert will visit Agents and branches as well.
- The frequency and scope of the review should be based on the risks specific to the business

Know Your Customer ("KYC")

MONEYTUN will comply with KYC guidelines issued by FinCEN and other applicable regulatory authorities, and will provide comprehensive training to its Employees and Agents on a regular basis. In furtherance of the KYC obligations, MONEYTUN has established due diligence procedures to ensure that the identity of its Customers and Agents is known.

KYC Procedures

- MONEYTUN's Employees must make every reasonable effort to determine the identity of each Customer as outlined in the Identification Requirements.
- MONEYTUN will not process any transaction that lacks required information.
- MONEYTUN's Employees must stay alert to unusual transactions or activities that are disproportionate to the Customer's known business or financial ability.
- Our Employees are critical to our Compliance program. MONEYTUN has established procedures to ensure that we know the identity of our Employees. MONEYTUN's Human Resources Department may also inquire when an Employee appears to be living beyond his/her known financial means, refuses to take vacation or habitually works during off-hours without apparent reasons.
- Employees may not have exclusive relationships with Customers or Agents. This is not intended to prevent typical Agent relationship.
- MONEYTUN has established due diligence procedures to ensure that it knows the identity of the Customers, Agents and Paymasters.
- All Agents and Paying Agents must be approved, prior to conducting business with MONEYTUN, by the Compliance Officer, and Credit Manager.
- Employees may not conduct transactions directly or on behalf of relatives without obtaining the prior approval of the Compliance Officer.

Identification Requirements

In furtherance of its KYC obligations, MONEYTUN requires its Employees to obtain information about the identity of each Customer by inspecting valid and acceptable identification, and to provide a copy to MONEYTUN's Compliance Officer when required *(see "MONEYTUN Transaction Processing").* .

Identification Acceptable for Individuals:

For individuals, "acceptable identification" means a form of unexpired, Government-issued identification with photograph, such as:

- A valid driver's license.
- A valid State issued non-driver identification card.
- A State-issued ID.
- A US issued work permit.
- A US issued alien registration card.
- A valid US or foreign passport.
- A Resident Alien card.

Identification Acceptable for Third-Party Transactions

It may be permissible for a Customer to conduct transactions through a third party. In this case, the Employee must obtain the following:

- Customer's full name, address and telephone number.
- Customer's valid and acceptable identification (as detailed above).
- Third Party's full name, address and telephone number.
- Third Party's valid and acceptable identification (as detailed above).

Unacceptable Identification

The following forms of identification are NOT acceptable:

- Food stamp card.
- Temporary or expired driver's license.
- Club and association cards.
- Check cashing cards.
- Marriage license.
- Library card.

- Business card.
- Fishing and hunting licenses.
- Social Security card*.

*Social Security cards may be used for identification.

Employee Compliance Guide

MONEYTUN must comply with legal requirements designed to detect and prevent money laundering and terrorist financing activities. This guide states what you must do to comply with MONEYTUN compliance policy. Failure to follow this guide violates MONEYTUN policy and may violate the law. Violation of this guide may result in termination of your employment. Violation of the law may result in criminal prosecution.

As a MONEYTUN employee, you have four compliance obligations:

1. Obtain and enter accurate information in the MONEYTUN system.

2. Identify your customer.

3. Do not assist structuring.

4. Report suspicious activities.

These obligations are not complicated, but it is essential that you understand what they are and comply with them fully. Each of your compliance obligations is explained below.

Obtain and Enter Accurate Information in the MONEYTUN System

At MONEYTUN, a number of the compliance activities are automated. For example, U.S. law requires that transfers of currency greater than $10,000 be reported to the government. These reports are generated automatically based on information entered in the MONEYTUN system and are filed by the MONEYTUN Compliance Department. In addition, the MONEYTUN system will prompt you to obtain and enter information that is required for compliance purposes.

REMEMBER: You must assure that accurate and complete information is entered in the MONEYTUN system.

Identify Your Customer

You must confirm that customers are who they say they are. A customer may transfer money on behalf of someone else. In this case, identification information is required for both the person making the transfer and the person on whose behalf the transfer is made. Identification information is required by the MONEYTUN system. Make sure that all required fields are

accurately completed and that any additional information requested by the MONEYTUN system is provided.

In addition,

- **For payment orders of $1,000 to $2,999:** you must review and input the valid and acceptable identification information in the MONEYTUN system: identification type, identification number, Issuing authority, expiration date.

    - **For payment orders of $3,000 and $4,999**: you must input the identification information in the MONEYTUN system and send to MONEYTUN Compliance Department a copy of one valid and acceptable government issued identification, the compliance form completed and signed by the customer. The compliance form must contain the Sender's Taxpayer Identification Number (such as Social Security Number or Employer Identification Number) or if none, must clearly state "None." Foreign issued passport should be obtained if the customer is neither a resident nor a citizen.

- **For payment orders in amounts between $5,000 and $9,999** must obtain or prepare (as applicable) the same information as required for transactions of $3,000 and up, ***plus***
    - One valid and acceptable form of identification.
    - A completed MONEYTUN BSA Compliance Form which must including, among other things, the Customer's occupation.
    - The compliance form must contain the Sender's Taxpayer Identification Number (such as Social Security Number or Employer Identification Number) or if none, must clearly state "None."
- **For payment orders of $10,000 and more:** must obtain or prepare (as applicable) the same information as required or transactions of $5,000 to $9,999, one valid and acceptable forms of identification, ***plus***

- If the Customer intends to fund the transaction in a form other than cash (i.e. check or wire) a copy of the form of payment.
  (Note: The BSA requires the Agent to keep copies of any such form of non-cash payment in addition to other forms of payment for at least 5 years from the date of the transaction), *plus:*

- A document evidencing the Customer's source of funds:
    - Any document that can adequately demonstrate the Customer's financial ability to conduct the transaction. In case there is an established customer a statement from the customer will adequately demonstrate the financial ability to conduct the transaction.

The foregoing documents and information must be submitted to the MONEYTUN Compliance Officer before the order will be released for payment to the Beneficiary.

Note: The BSA requires MONEYTUN to file a Currency Transaction Report (FinCEN Form 104) for any transaction or a series of transactions by a single Customer totaling more than US$10,000 in one day.

Identification is valid if it has not expired and has not been cancelled or revoked. Review the identification to verify that the expiration date has not passed. An identification that has been cancelled will usually have holes punched in it or be stamped to show that it is no longer valid.

REMEMBER: Provide all information required about the customer and the recipient by the MONEYTUN system, make sure that any identification required is both valid and acceptable and provide a copy of any required identification to MONEYTUN Compliance Department and place a copy together with the copy of the transaction receipt in your files for future reference.

Do Not Assist Structuring

It is illegal to break or fraction a transaction into two or more smaller transactions to avoid regulatory requirements. This practice is called "structuring". For example, a customer who asks you to transmit $10,000 in two transactions of $5,000 each is engaged in structuring. There may be reasons why this may not be structuring such as when a foreign paying bank is restricting how much could be paid out in a day. In addition, customers can structure to avoid the $3,000 reporting requirement. It is also illegal under structuring regulations to tell customers what regulatory reporting and identification requirements are. For example, you may not tell a customer that transfers greater than $2,000 fall under BSA regulatory thresholds. If you believe a customer is attempting to structure a transaction you must report it as a suspicious transaction.

REMEMBER: Never discuss reporting, identification or other regulatory requirements with customers and never suggest that a customer break a transaction into separate transactions.

Report Suspicious Activity

A transaction is suspicious if it appears

- To involve unlawful activity
- To serve no legitimate purpose
- To be structured to avoid a reporting requirement

Examples of suspicious activity include:

- Altering a transaction to avoid completing a funds transfer record ($3,000 or more),
- Altering a transaction to avoid regulatory reporting (more than $10,000),
- Changing spelling or arrangement of a name,
- Using false identification documents,
- Two or more persons using the same or similar identification,

- Offering a "tip" or other compensation to an employee in connection with a transaction.

If you see suspicious activity you must complete and send to MONEYTUN a "Suspicious Activity Report Form" (SAR). You must not tell a customer that you suspect suspicious activity or that you will file a SAR.
REMEMBER: You must be alert for suspicious activity and report suspicious activity to MONEYTUN compliance department along with supporting documents. The compliance department will then determine whether filing of a SAR is warranted.

Sending Documents and Asking Questions

Copies of required identification and SAR Forms should be sent by email to MONEYTUN Compliance Department.

If you have questions about compliance, call the MONEYTUN Compliance Department or send an e-mail to arthur@moneytun.com

Prohibited Conduct

Structuring

It is a felony for a Customer or a group of Customers to split a transaction into smaller transactions of US$10,000 or less in order to evade or cause to evade the filing of the Currency Transaction Report ("CTR") or other BSA recordkeeping requirements. This crime is called *"Structuring"*. You become a participant, and guilty of a crime, if you knowingly assist someone in structuring or advice or conspire with someone on how to evade the law.

Structuring is not limited to multiple transactions on the same day. It includes those conducted over one or more days if done to evade the BSA reporting requirements. For example, if a Customer regularly, on consecutive or near consecutive days, conducts cash transactions of less than US$10,000 but which collectively add up to $10,000 or more, there is a strong likelihood they are structuring. Please note that structuring can be done to avoid the $2,000 SAR filing requirement or the $3,000 recordkeeping requirement.
Under no circumstances may any Employee, Agent or Agent's employee advice or instruct Customers on grouping or structuring transactions to avoid a CTR, recordkeeping requirement or SAR filing requirement.

MONEYTUN employs a technique called "aggregation" which involves the analysis of all its transactions over various periods of time across all of its Customers and locations in order to determine whether structuring is occurring. MONEYTUN devotes considerable resources to this process.

It is also MONEYTUN's policy to aggregate transactions across all products in order to maximize detection of suspicious transactions and to ensure that CTRs are appropriately filed for transactions in amounts of more than US$10,000.

Suspicious transactions

A suspicious transaction is one or more transactions:

- That involve funds derived from illicit activity and is intended or conducted in order to hide or disguise the illicit funds **or**
- Designed to evade the BSA requirements, whether through structuring or other means **or**
- Appeared to serve no business or apparent lawful purpose (and MONEYTUN and its agents can determine no reasonable explanation for the transaction after examining the available facts).

Examples include:

- Patterns of repetitive payment orders that do not appear to have any business purpose.
- Other transactions that appear to have no business purpose, or are unusual or non-typical for the Customer.
- Transactions by Customers who are unwilling to provide the required information.
- Transactions just below the identification requirement threshold.
- Transactions by Customers who are overly inquisitive as to BSA reporting requirements.
- Transactions known or suspected to be designed to evade MONEYTUN's recordkeeping duties, or any other BSA requirement, whether through structuring or other means.
- Transactions involving money from criminal activity.
- Transaction intended to use the money services business to facilitate criminal activity.

If you become aware of suspicious activity by any Agent or any Agent's Customers, you must promptly report the matter to the MONEYTUN' Compliance Officer using a Suspicious Activity

In connection with the preparation and filing of SAR-MSBs, all Employees and Agents are required to cooperate with MONEYTUN's Compliance Officer in obtaining and providing any information he or she requests on a timely basis.

Whenever suspicious activity is deemed serious or could potentially involve terrorist activities, the employee and/or agent must complete the suspicious activity report referral form and send it to the MONEYTUN compliance officer immediately.

Disclosure of a Suspicious Activity Report ("SAR-MSB") Filing

It is illegal to notify or advise anyone who is the subject of a SAR-MSB filing. It is also illegal to discuss any potential or actual SAR-MSB filing with anyone, including relatives and/or acquaintances, other than those individuals within MONEYTUN who have a 'Need to Know'.

Therefore, it is MONEYTUN's policy that the filing of a SAR-MSB must be kept in the strictest of confidence.

Any person subpoenaed or otherwise requested to disclose a SAR-MSB filing, or the information contained in a SAR-MSB, must decline to produce the information and must direct the inquirer to the MONEYTUN Compliance Officer.

If a Customer or potential Customer inquires about the SAR-MSB process, or if applicable, the reasons behind MONEYTUN's refusal to transact with the individual, the Employee and/or Agent must inform the individual that he/she is **"not permitted to provide this information"** If the individual persists, the Employee and/or Agent should contact the MONEYTUN Compliance Officer, who will determine whether the Customer or potential Customer is exhibiting behavior that might be considered suspicious, potentially resulting in the filing of a SAR-MSB. The BSA has a "Safe Harbor" provision granting MONEYTUN and its Agents immunity from any lawsuit filed Customer as a result of being identified in a SAR-MSB filing.

Regulatory Filings

Currency Transaction Report ("CTR")

The BSA requires that MONEYTUN file a CTR Form 104 when a transaction or a series of transactions are conducted by the same person or on behalf of the same person involving currency totaling more than US$10,000. The CTR must be filed with the appropriate office of the US Treasury no later than 15 days from the date of the transaction. MONEYTUN will file all required CTRs on behalf of its Agents.

The Agent or Employee entering the transaction is required to provide the MONEYTUN Compliance Officer with the completed MONEYTUN BSA Compliance Form and all supporting information; not only on an individual transaction which is US$10,000 or more, but also at any time there are multiple transactions by or on behalf of the same Customer in any one day totaling US$10,000 or more.

If we receive and/or disperse currency, we will file with FinCEN CTRs for transactions involving currency that exceed $10,000. Multiple transactions will be treated as a single transaction if they total more than $10,000 during any one business day.
We will use the publicly accessible website -https://bsaefiling1.fincen.treas.gov/PublicAccess for all our CTR filings as of September 1st 2012. Printed records of all filled CTRs will be retained by the compliance officer for five (5) calendar years.

It is a policy of Moneytun LLC that all CTRs should be filed within 15 calendar days of the reported transaction(s) as required by Federal Regulations. A Compliance officer should execute weekly aggregated transaction reports (Frequency reports), to detect and identify transactions above $10,000 threshold for CTR filings. All CTRs will be filed by Moneytun LLC's main office and signed by a Chief Compliance Officer.

The following are examples of situations requiring a CTR filing:

- Mr. A wants to send $9,950 to someone in Costa Rica and along with the $51 fee, the total amount of cash given by the Customer is $10,001.
- Mrs. M. brings $12,000 in cash, she wants to send $4,000 to someone in Brazil and $8,000 to someone in Argentina. Because the total is $10,000 or more, a CTR must be completed.

Suspicious Activity Report ("SAR-MSB")

After a review of all available information, MONEYTUN will file a SAR-MSB whenever MONEYTUN or a MONEYTUN Agent believes that a transaction or patterns of transactions are suspicious, regardless of the amount. Please note that to file a SAR the suspicious activity of the customer must be $2,000 or more.

SAR-MSBs are due no later than 30 calendar days from the date of initial detection by MONEYTUN of facts that may constitute a basis for filing. In situations involving violations that require immediate attention, such as, for example, ongoing money laundering schemes, MONEYTUN will immediately notify, by telephone, an appropriate law enforcement authority in addition to timely filing a SAR-MSB.

If a currency transaction is more than US$10,000 and is suspicious, MONEYTUN must file both a CTR and a SAR-MSB. If a currency transaction is less than US$10,000 but is suspicious, MONEYTUN is only required to file a SAR-MSB.

As a MONEYTUN Employee, you must report all suspicious transactions to the **MONEYTUN Compliance Department**.

If MONEYTUN does not file a required SAR-MSB due to employee failure to report a suspicious transaction to MONEYTUN, a Federal agent or prosecutor may later conclude that the employee was 'willfully blind'[1] to illegal activity.

As with CTRs, MONEYTUN employs multiple layers of review and responsibility in order to reduce the likelihood of missing a required SAR-MSB filing:

[1] 'Willful blindness' is a legal principle that has been used to convict persons for participating in crimes where their only involvement was conducting the transaction and not reporting something which should have been considered suspicious.

A. Where the transaction originates at an Agent, the Agent has the first level of responsibility for obtaining all required information to complete the SAR-MSB. Although MONEYTUN ultimately files each SAR-MSB, MONEYTUN should receive a copy of the MONEYTUN BSA Compliance Form and all required documentation from the Agent.

B. When an Employee concludes that a transaction or series of transactions require SAR-MSB, the Employee is responsible for: (1) Obtaining a completed BSA Compliance Form from the Agent or Employee who initiated the payment order(s), (2) retrieving copies of the appropriate IDs, (3) completing the SAR-MSB and (4) submitting the completed SAR-MSB and supporting information to the MONEYTUN Compliance Officer for review and filing.

C. The MONEYTUN System stops all orders that aggregate to US$3,000 or more for manual inspection by a Compliance Employee in order to determine whether the transactions are being structured to avoid the record keeping or the reporting requirements and that proper evidence of ID and required information is provided by the customer.

D. On a weekly basis, designated Compliance Employee, conducts an aggregated report of transactions of $3,000.00 and above in order to determine if possible structuring has taken place The Transaction Frequency Report (TFR) then sent to MONEYTUN'S compliance officer for review and signature. Where appropriate, CTRs and/or SAR-MSBs will be filed.

E. On a bi-weekly basis, designated Compliance Employee should conduct post-transactional review of all transactions of $2,500 and more to ensure that no report was inadvertently omitted. If any such omission is discovered, it is to be reported immediately to the MONEYTUN Compliance Officer who will:

- Arrange for prompt filing of the omitted report; and
- As promptly as practicable, determine the cause of such omission and take any necessary corrective or disciplinary action.

Reporting To the Office of Foreign Asset Control ("OFAC")

Before engaging in any money service activity (including but not limited to check cashing, money orders and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website (s*ee* www.treas.gov/offices/enforcement/ofac/sdn/index.html).

Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists

through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, 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 business days.
We may also call the OFAC Hotline at **1-800-540-6322**.

Checking the Office of Foreign Assets Control (OFAC) Lists

Before engaging in any money service activity (including but not limited to check cashing, money orders and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website (s*ee* www.treas.gov/offices/enforcement/ofac/sdn/index.html).

Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, 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 business days.
We may also call the OFAC Hotline at **1-800-540-6322**.

Agent management and oversight

Agent recruitment

Agents come to MONEYTUN in one of two methods. Solicited agents are those who have come to the attention of, and are then approached by MONEYTUN, to become part of the

agent network. Unsolicited agents are those who approach MONEYTUN, seeking to contract with MONEYTUN to become part of the agent network.

In contracting an agent, MONEYTUN has an implicit responsibility to know that the agent, as an extension of MONEYTUN, is worthy of being entrusted with the funds remitted by MONEYTUN's customers. Second, MONEYTUN must ascertain that the agent will not willingly or unwittingly engage in activities that result in BSA violations.

To meet its first responsibility, MONEYTUN has adopted a policy to conduct enhanced due diligence reviews on its potential agents prior to signing contracts with those entities. When possible, in addition to the signed contract and a fully completed application, MONEYTUN may:

- Conduct credit checks on the agent-company's principal.
- Determine how long applicant has been in business
- Obtain agent's principal's identification
- Inquire whether the agent's principal has pending or resolved criminal convictions (conduct criminal background checks).
- Determine whether any licenses or permits have been revoked from the principals of the agent-company
- Verify status of agent's business entity
- Review lease documents
- Verify agent's telephone numbers
- Review utility invoice
- Obtain picture of the agent's store front
- Conduct periodic updates of the above information

MONEYTUN will conduct an independent investigation of the applicant's credentials. This information may include reports on the potential agent's ownership structure, income, assets, net worth, and required business registration will be maintained in the agent's file. Thereafter, on an annual basis, or when changes in circumstances come to MONEYTUN's attention, the records will be updated.

To meet second responsibility, that is that agents will comply with the anti-money laundering and BSA requirements, MONEYTUN will instruct and train its agents about MONEYTUN's policy to ensure they are aware of the legal requirements imposed by the BSA and other anti-money laundering laws, and of the latest schemes used to launder money through businesses such as MONEYTUN. In further fulfilling its obligations MONEYTUN will periodically stress-test the agents' knowledge and application of BSA and anti-money laundering principles. Independent testers may be used to ensure compliance, and tests will be conducted without the prior consent or knowledge of the agent. Additionally, MONEYTUN will advise agents to contact the Compliance Officer concerning all BSA and anti-money laundering related issues or questions. A direct line of communications must always be maintained between the agents and the Compliance Department to ensure complete adherence to MONEYTUN's compliance policy.

Agent supervision and training

After successfully screening the agent, MONEYTUN's responsibility then becomes managing that agent. While the agent is authorized to either receive or pay remittances on behalf of MONEYTUN, MONEYTUN has a responsibility to ensure that the agent is doing so without violating the law. As the gateway to MONEYTUN's financial services infrastructure, the agents play a pivotal role in ensuring that MONEYTUN is not used as a conduit for laundering funds.

MONEYTUN's primary tools to ensure compliance are training and mystery shopping. An agent and its employees are not expected to guess at what the laws require. Rather, MONEYTUN will use various methods to inform the agent what legal requirements apply to the agent as a Financial Institution. MONEYTUN will also monitor each agent's transactions to ensure compliance.

Agent termination and relocation

The process for terminating agents is as important as the hiring and the supervision of agents. Usually, the termination of agents results in a report being made to the Department of Financial Institutions of the state where the agent is located. The Compliance Officer is charged with timely and effectively communicating this information to those entities.

Additionally, the Compliance Officer must ensure that the agent is removed from the list of currently active agents which MONEYTUN must maintain pursuant to FinCEN regulations. Importantly, the Compliance Officer must take care to keep the agent's corporate and personal information for at least 5 years from the time of termination.

From a practical perspective, the termination process ends with MONEYTUN's collection of all outstanding, unused receipts bearing MONEYTUN's name. Depending on the specific circumstances of the termination, and often State law or regulation, MONEYTUN may provide written notification of the agent's termination to all users of MONEYTUN's services who used that agent in the previous year. This provides notice to those users that MONEYTUN's relationship with the agent is officially ended.

As important as it is for agents to "know" their customers, it is equally important for MONEYTUN to "know" its agents. Agents represent the largest compliance risk for money transmitters and can facilitate laundering funds by simply misapplying their knowledge or their privileged position as insiders. Because of the ever-present risk that agents may willingly or unwittingly assist in the laundering of funds, it is imperative that MONEYTUN maintain a strict policy of "knowing" its agents ***before*** those agents are contracted.

After they are signed as agents, MONEYTUN has a continuing obligation to know how the agents are discharging their regulated and fiduciary role. Equally important is the process MONEYTUN uses for terminating the agency relationship. In summary then, with respect to agents, MONEYTUN has a three-fold responsibility: recruiting agents; supervising and training agents while they are active; and termination.

Correspondent Paying Agents

Correspondents, or paying agents, are Financial Institutions by U.S. definition because if they were organized in the U.S. and conducted the services in the U.S., they would be required under Section 352 of the USA PATRIOT ACT to maintain an anti-money laundering compliance program.

As a result, MONEYTUN must adopt policies, procedures and controls concerning foreign correspondents and foreign paying agents that permit MONEYTUN to:

- Assess whether the correspondent presents a significant risk of money laundering
- Consider information available from US governmental agencies and multinational organizations with respect to supervision and regulation, if any, applicable to the correspondent
- Review guidance issued by the Treasury Department regarding money laundering risks associated with correspondents or Foreign Financial Institutions generally; and
- Review publicly available information to determine whether the correspondent or the foreign paying agents (or its owners) have been the subject of criminal action of any nature, or regulatory action related to money laundering.

Under MONEYTUN's requirements, before agreeing to contract with a correspondent or foreign paying agents, MONEYTUN will do the following:

- Determine if the correspondent is duly incorporated as a business in the country where it will pay
- Maintain current copies of all licenses and permits required to conduct the businesses.
- Maintain copies of the list of shareholders of the correspondent's owner(s).
- Maintain information about the banks and bank account numbers used by the correspondent.
- Maintain a list of all the countries from where the correspondent receives payments and where it sends remittance orders to be paid
- Maintain copies of the latest financial information if possible.
- Maintain copies of the correspondent's compliance program, including a detailed description of how the correspondent complies with the anti-money

laundering controls of the correspondent's country and those of the United States for transactions that originate or are paid in the United States.

- If possible, conduct physical visits when the correspondent relationship is created and thereafter no later than every two years to ascertain that the correspondent has a physical location, employees and an infrastructure adequate to conduct the business of correspondent on behalf of MONEYTUN.
- Require that MONEYTUN be informed about any material changes in any aspect of the correspondent's business, including any changes in address, changes in ownership, establishment of other business or products, expansions of correspondent's branches, or any changes in the financial status of the business or any of its owners.
- Review any available public information about the correspondent
- Consult government advisories or information concerning the correspondent in particular and foreign financial institutions in general
- Review the recommendations of the Financial Action Task Force (FATF), FinCEN and the financial intelligence agencies of the country where the correspondent operates.

Branches and Agents Audit

The purpose of the agent and branch audit program is to strengthen MONEYTUN's compliance program and mitigate the risk of being utilized as a conduit of illicit funds, money laundering and/or terrorist financing.

Working through independent agents creates an inherent risk due to the agents' lack of controls, training deficiencies and employee turnover. Implementing an aggressive agent and branch audit program will help identify regulatory, training, money laundering, and terrorist financing risks.

Risk Assessment.

Compliance risk is the risk of violations of, or non-conformance with, laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk is also the possibility that MONEYTUN could be utilized as a conduit of illicit funds or funds for terrorism financing. Compliance risk exposes MONEYTUN to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, lessened expansion potential, and lack of contract enforceability.

MONEYTUN is in the business of money transmission for mostly migrant workers that send money back to their families in their country of origin. The business is conducted through appointed independent agents, and branches.

As a regulated entity MONEYTUN is required to comply with the Bank Secrecy Act, the USA Patriot Act, OFAC and laws and regulations of the jurisdictions it operates. For the most part, in particular federal law that apply to documentation, reporting, training, independent audit and internal controls to prevent money laundering and/or terrorist financing are incorporated by reference by the state jurisdictions where MONEYTUN operates.

MONEYTUN has established a compliance program to comply with the regulatory requirements both at the federal and state levels. Agents and branches audit substantially enhances MONEYTUN's ability to identify and mitigate risks.

Due to the nature of MONEYTUN's business the following areas create risks that need to be identified and mitigated in order to be in compliance with the regulatory scheme. The risk rating model will incorporate factors from the following areas:

Origination of the transaction
- Agent Location
- Agent that originates the transaction
- Agent's customer base
- Agents transaction volume
- Agents transaction principal volume
- Regulatory compliance requirements where the agent is located
- Money laundering risk where the agent is located

Destination of the transaction
- Paying agent
- Beneficiary location
- Money laundering and or terrorist financing risk where the beneficiary is located
- Regulatory compliance requirements where the beneficiary is located

Risk Rating Model

The risk rating model will evaluate the factors for the different areas of risk and assign individual factors values from one (1) to five (5); five being the highest risk.

Once the individual factors are assigned a value the total risk score is calculated by adding the factors values. **The highest risk score is 20**

Assumptions for risk rating:

Agent location:

Large cities are assigned a score of four (4)
Large cities are Chicago, Miami, Houston, Dallas, Tucson, Phoenix, St Louis, Atlanta, Boston, Seattle, and San Francisco.

High risk cities are assigned a score of five (5)
High risk cities are Los Angeles, New York City, Puerto Rico, and Westminster

All other cities are assigned a score of three (3)

Destination:

The country of destination is assigned a risk score based on the perceived risk for money laundering and/or terrorist financing.

Number of Transactions:

Based on the number of transactions the following scores will be assigned:

Less than 200 transactions per month a score of 1
Less than 500 transactions per month a score of 2
Less than 800 transactions per month a score of 3
Less than 1200 transactions per month a score of 4
Greater than 12000 transactions per month a score of 5

Average transaction

Average transaction compared with MONEYTUN's average transaction

Less than 350 a score of 1
Less than 450 a score of 2
Less than 550 a score of 3
Less than 650 a score of 4
Greater than 650 a score of 5

Once the agent's risk is established, the agents with the highest scores will be scheduled for additional training and close monitoring or audit visits and mystery shopping.
:

Training For Employees & Agents

All Employees and Agents of MONEYTUN share in the responsibility of ensuring adherence to MONEYTUN's commitment to Compliance. To that end MONEYTUN has developed and implemented a training program that requires every employee and agent to be trained as follows:

1. Every new employee must be trained on MONEYTUN's compliance policies and procedures before the employee commences work.
2. Every new agent must be trained on MONEYTUN's policies and procedures before the agent is activated and starts operating as an authorized agent.
3. The employees and agents must be retrained on a regular basis going forward and as required by changing laws and regulations

The training program will incorporate the requirements of the Bank Secrecy Act, the USA Patriot Act, the Anti-Money laundering laws, and other applicable federal and state laws and regulations.

Moneytun has developed ongoing employee training under the leadership of the AML Compliance Officer. Our training will occur on at least an annual basis. Based on our firm's size, its customer base, and its resources we have determined that Exchange Analytics, Inc. will provide the training course to our staff. The course is administered online at https://www.tamlo.com

The training course offered by Tamlo includes, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act. The training program offered by Exchange Analytics, Inc. includes the maintenance of the records to show the persons trained, the dates of training, and the subject matter of their training.

Training will be provided in lieu of the Tamlo's online course, which will also include in-person lectures and explanatory memos as necessary. Logs of provided training should be maintained, which should include the following information: a) date of ANY training conducted; b) Detailed information on the material covered; c) List of attendees whom compelled the AML training as required by BSA regulations.

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.

Mystery Shopping

The purpose of MONEYTUN's Mystery Shopping Program is to support MONEYTUN's legal obligation to maintain internal controls to prevent and detect illegal acts by MONEYTUN employees and MONEYTUN agents. The Mystery Shopping Program also serves as a metrics tool used to quantify Agent's Risk and measure level of training and monitoring required.
The Program sends undercover operatives to branches and agencies posing as customers to attempt to conduct a transaction in a way that will persuade the MONEYTUN employee or agent to accept the transaction while either avoiding the documentation requirements, violating MONEYTUN's policies and procedures, failing to report the transaction, or failing to refer suspicious behavior.

MONEYTUN has only one agent and presently there is no need for Mystery Shopper Program. If in the future MONEYTUN decides to engage the services of many agents then it must develop Mystery Shopper program.

Recordkeeping

MONEYTUN will retain all records for at least 5 years, as required by the Secretary of the Treasury under the BSA (31 CFR 103.38)), including original, copies or other appropriate records of the following items:

- Daily sales records and supporting documents.
- Each item of cash or checks in excess of $10,000 remitted or transferred out of the United States.
- CTRs filed and supporting documentation.
- SARs filed and supporting documentation.
- Bank account statements and supporting records.
- Training programs, materials, and attendance records.
- Board of Directors Meeting Minutes, including any sub-committees.
- KYC documentation, including Risk Rating and profiling records for all applicable customers.
- Information and identification requirements for transaction of US$3,000 or more
- Any other documentation required by local, State, or Federal regulatory authorities.

MONEYTUN will keep a full **and accurate** record of each transaction or attempted transaction that is subject to the provisions of 31 CFR 500-575.601 (Foreign Asset Control Regulations "OFAC"), regardless of whether such transactions were effected pursuant to an OFAC license. Unless OFAC regulations provided for longer periods, MONEYTUN will retain OFAC-related records for at least 5 years.

Documents no longer required to be retained by this Section will be disposed of in accordance with MONEYTUN's Records Retention and Destruction Policy as in effect from time to time. All disposition inventory records, reviews undertaken and evidence of supervision of disposition will be maintained for a minimum of 5 years (or such longer period as may be required by MONEYTUN's Records Retention Policy).

Responding to Inquires from Law Enforcement and other Government Officials

It is possible that a financial institution will receive a number of different types of formal written legal communications. In addition, government personnel may engage in informal communications with financial institutions. In advance of issuing legal process for the production of records, documents or other information, law enforcement and other government personnel may contact financial institutions as a courtesy and in some cases to narrow the scope of the subpoena or summons.

Infrequently, a government representative may ask that records, documents or other information be produced without the benefit of a subpoena, summons, or other legal process. To protect MONEYTUN customers, MONEYTUN requires legal process prior to production or disclosure of records, documents and other specific information.

If MONEYTUN is served with a subpoena, summons, search warrant, or other legal process, or if a government agency otherwise requests information or documents involving the BSA, money laundering or terrorist activity, the MONEYTUN Compliance Officer must be contacted immediately.

Only the MONEYTUN Compliance Officer and other MONEYTUN officers and employees who have been authorized by the MONEYTUN Compliance Officer and the General Manager, are authorized to respond to legal process, legal notices, or other inquiries received from law enforcement or other government authorities or otherwise communicate with law enforcement officials or with other government authorities with respect to criminal and other legal matters related to the BSA, the money laundering and anti-terrorism statutes, and related criminal matters.

Written inquiries, including legal process, seizure notices and forfeitures notices, involving the BSA, money laundering, terrorism or other criminal activity which are received by MONEYTUN officers and employees must be hand delivered the same day to the MONEYTUN Compliance Officer. If the written inquiry received by MONEYTUN is legal process directed to MONEYTUN, such legal process shall be faxed the same day as received by the MONEYTUN Compliance Officer to MONEYTUN counsel.

The original legal process document(s) addressed to MONEYTUN shall be sent the same day by overnight mail or express courier to the counsel. Telephone inquiries received by MONEYTUN officers and employees must be transferred immediately to the MONEYTUN Compliance Officer or his or her designee.

MONEYTUN officers and employees shall respond in a timely fashion to each request for assistance from the MONEYTUN Compliance Officer or counsel. All documents and other information requested by the MONEYTUN Compliance Officer or counsel shall be provided to the MONEYTUN Compliance Officer or counsel within the time period specified by MONEYTUN Compliance Officer or counsel. The MONEYTUN Compliance Officer or counsel must respond to each lawful request received from a law enforcement official or other government agency within the time period specified in the request unless the time period has been extended in writing.

A written record will be made of all telephone and other verbal inquiries from government officials. Each record will include the name and title of the government official making the inquiry, the name of the government agency, the telephone number of the government official, the name and telephone number of the MONEYTUN employee receiving the inquiry, a summary of the inquiry, and the action taken with respect to the inquiry.

Neither the MONEYTUN Compliance Officer nor counsel shall provide responsive information to any telephone inquiry or oral request for information unless the request is followed by a proper subpoena, other legal process or appropriate written request. Records of telephone calls and other verbal inquiries from government officials will be maintained by the MONEYTUN Compliance Officer in a designated file for a period of at least five years. Records of calls not initially received by the MONEYTUN Compliance Officer must be forwarded to the MONEYTUN Compliance Officer for recordkeeping.

A written chronological "Subpoena/Official Request Log" shall be maintained by the MONEYTUN Compliance Officer. With the exception of Section 314(a) Requests, the Subpoena/Official Request Log shall contain an entry of each subpoena, summons, search warrant or other legal process or written request received from a government official relating to possible BSA violations, money laundering, terrorism, or other criminal activity. Section 314(a) Requests shall receive special handling as described below.
The Subpoena/Official Request Log shall contain the following information:

- the date of receipt by MONEYTUN;
- the due date (if any);
- the type of legal process or written request received;
- the federal, state or local or foreign government agency responsible for the subpoena, other legal process or written request;
- the city in which the agency is located;
- a summarized description of the documents and other information requested; and
- the date(s) MONEYTUN responded to the request.

Subpoena/Official Request Log entries will be maintained by the MONEYTUN Compliance Officer for a period of at least five years from the date of final response to the subpoena, other legal process or written request in a designated Subpoena/Official Request Log file.

In addition to maintaining a Subpoena/Official Request Log, a separate individual Subpoena/Official Request File shall be created for each subpoena, other legal process or

written request received that relates to possible violations of the BSA, money laundering or terrorism statutes, and other criminal activity. Upon receipt of a subpoena, other legal process or written request, the MONEYTUN Compliance Officer, in coordination with counsel, shall evaluate the request and the time frame for response.

In those cases where production documents, records or other information is requested and legal process is not received, the MONEYTUN Compliance Officer must determine whether the type and nature of the request requires a subpoena or other proper legal process. In cases where the request relates to specific transactions or persons, legal process generally should be required. In those cases, the MONEYTUN Compliance Officer or counsel shall contact the government authority making the request to ask that MONEYTUN be served with proper legal process. In such cases, MONEYTUN shall not respond to the request unless and until proper legal process is received.

In some cases it may be necessary to narrow the scope of the subpoena, other legal process or written request, or to obtain an extension of time to respond. In such cases, the MONEYTUN Compliance Officer or counsel shall contact the responsible government official to discuss the subpoena, other legal process or written request and try to narrow its scope or obtain an extension of time for response. A written record of each contact with government authorities will be made and kept in the file relating to the particular Subpoena/Official Request.

If the scope of the subpoena or other legal process is narrowed or an extension is obtained, the MONEYTUN Compliance Officer must send a letter to the responsible official confirming the agreement and maintain a copy of the confirmation letter in the Subpoena/Official Request File. If the MONEYTUN Compliance Officer is unable to reach an agreement with the government agency with respect to the scope of the subpoena or other legal process, or obtain an extension, the MONEYTUN Compliance Officer shall notify immediately the counsel for appropriate guidance. The counsel shall take appropriate action including moving to quash the subpoena or other process.

The MONEYTUN Compliance Officer shall reply in writing to each subpoena or other lawful legal process and, in appropriate cases only, to a written request received relative to the BSA, money laundering or terrorist activity.

The written reply shall include: (i) a cover letter; (ii) a copy of the original subpoena, other legal process or written request; (iii) a copy of any subsequent modification to the original subpoena, other legal process or written request; and (iv) each document provided in response to the subpoena. A complete copy of each written reply, including each document provided in response to the subpoena, other legal process or written request, will be maintained in the Subpoena/Official Request File. Each reply will be sent to the responsible government official either by certified mail, by overnight mail or by courier and the certified mail, overnight mail or courier receipt will be kept in the Subpoena/Official Request File. Each Subpoena/Official Request File will be maintained by the MONEYTUN Compliance Officer for a period of at least five years from the date the last document is provided to the government in response to the subpoena, other legal process or written request.

Section 314(b) Registration

The BSA, as amended by Section 314(b) of the USA Patriot Act, authorizes financial institutions to share information with other financial institutions or associations of financial institutions regarding individuals, organizations and countries for purposes of detecting, identifying or reporting activities that the financial institution suspects may involve possible money laundering or terrorist activities. To share information under the BSA a financial institution must file annually a specific notice with FinCEN and comply with requirements relating to verification, use and security of information. A financial institution that follows the BSA procedure for voluntary sharing of information is afforded immunity from civil suit by an individual or entity that is identified in any such sharing of information request or response.
MONEYTUN information shall be shared with other financial institutions as instructed by the MONEYTUN Compliance Officer.

The MONEYTUN Compliance Officer is the designated point of contact for information sharing with other financial institutions by MONEYTUN.

The MONEYTUN Compliance Officer shall submit a notice to FinCEN ("314(b) Notice") indicating the intent of MONEYTUN to share information. The 314(b) Notice shall include the following: the name of MONEYTUN as the financial institution that intends to share information, the taxpayer identification number (TIN) of MONEYTUN; the primary mailing address of MONEYTUN, the name of the contact at the financial institution (i.e., the name of the MONEYTUN Compliance Officer), the contact's title, the contact's e-mail address, and the phone and fax number of the contact. By submitting the 314(b) Notice, the financial institution makes specific commitments contained therein with respect to safeguarding the confidentiality of any information shared.

MONEYTUN shall maintain adequate procedures to protect the security and confidentiality of information received under 314(b).
If, as a result of information shared, MONEYTUN knows, suspects, or has reason to suspect that an individual, entity, or organization is involved in, or may be involved in, terrorist activity or
money laundering, or other criminal or suspicious activity the MONEYTUN Compliance Officer shall file a Suspicious Activity Report on the suspect or suspects.
With respect to matters requiring immediate attention, such as terrorist activity or an ongoing money laundering violation, the MONEYTUN Compliance Officer immediately shall notify, by telephone, an appropriate law enforcement authority. In the case of terrorist activity, a report shall be made to the Financial Institutions Hotline at 1-866-556-3974. In the case of money laundering, a report shall be made to office of the IRS CID nearest to the Agent location which is the site of the activity being reported. For each matter reported telephonically, regardless of amount, the MONEYTUN Compliance Officer shall file a Suspicious Activity Report.

Privacy Policy and Notice (Gramm-Leach-Bliley Act)

Pursuant to the requirements of Title V of the Gramm-Leach-Bliley Act MONEYTUN Financial Holdings Inc., and its related companies ("MONEYTUN") do not disclose any non-public personal information obtained during the course of processing the money remittance orders, about customers or former customer to anyone, except as permitted or required by law and as required to process the money transmission order in accordance with the customer's instructions.

REGISTRATION AS A MONEY SERVICES BUSINESS (MSB).
It is the policy of MONEYTUN to register as an MSB. MONEYTUN will use the **Revised RMSB Form 107 for Money Services Business Registration which became Effective September 1, 2008.**
Effective September 1, 2008, a Money Services Business is required to use the revised FinCEN Form 107, Registration of Money Services Business (RMSB) to register its business. FinCEN announced in April 2008 that it was revising the RMSB Form 107. This change is required to incorporate the **five (5) critical fields that are now mandatory for a registration to be accepted (Legal name, Address, City, State, and EIN (entity) or SSN/ITIN (individual**)). **All previous versions of Form 107 will not be accepted after December 31, 2008.**

MONEYTUN will prepare and maintain a list of agents - must be completed in conjunction with the initial registration. Information about the agent volume must be current within 45 days of the due date of the agent list.

MONEYTUN will update the agent list on January 1 of each year - information about the agent volume must be current within 45 days of the due date of the agent list. MONEYTUN will comply with all other requirements of the Revised RMSB Form 107.

Foreign Bank Account Report (FBAR)

An FBAR is a Report of Foreign Bank and Financial Account. The form number is TD F 90-22.1 (PDF). Any United States person who has a financial interest in or signature authority, or other authority over any financial account in a foreign country, if the aggregate value of these accounts exceeds $10,000 at any time during the calendar year must file. A "foreign country" includes all geographical areas outside the United States, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the territories and possessions of the United States (including Guam, American Samoa, and the United States Virgin Islands).

A person has signature authority over an account if such person can control the disposition of money or other property in it by delivery of a document containing his or her signature (or his or her signature and that of one or more other persons) to the bank or other person with whom the account is maintained. Other authority exists in a person who can exercise power that is comparable to signature authority over an account by direct communication to the bank or other person with whom the account is maintained, either orally or by some other means.

The FBAR is due by June 30th of the year following the year that the account holder meets the $10,000 threshold. The granting, by IRS, of an extension to file Federal income tax returns does not extend the due date for filing an FBAR. There is no extension available for filing the FBAR.
If an account holder does not have all the available information to file the return by June 30th, they should file as complete a return as they can and amend the document when the additional or new information becomes available. FBAR forms are available: On the IRS.gov (PDF) Web site.

Sharing AML Information with Federal Law Enforcement Agencies and Other Financial Institutions

Under the U.S. Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to any FinCEN request about accounts or transactions 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 FinCEN's request. Upon receiving an information request, the AMLCO is to be responsible regarding the request and similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts and transactions, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form in a timely manner. If we search our records and do not uncover a matching account or transaction, then we will not reply as allowed under Section 314(a) of the PATRIOT Act.

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. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, as required by Section 501 of the Gramm-Leach-Bliley Act. We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the Company in complying with any requirement of Section 314 of the PATRIOT Act.

Sharing Information with Other Financial Institutions under Section 314(b)

We will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that

may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file an initial notice with FinCEN before any sharing occurs and annual notices afterwards. We will use the notice form found at http://www.fincen.gov/fi_infoappb.html or use a paper notification mailed to FinCEN, P .O. Box 39,Mail Stop 100, Vienna, VA 22183 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 with respect to financial institutions with whom we are affiliated, and so 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, including segregating it from the firm's other books and records.

Code of Conduct

It is the Company's Policy that each Employee shall read and understand the AML policy and AML Program and certify to the same. Each employee should also read and understand the Code of Conduct of the Company and certify the same.

Additional Areas of Risk

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and is continually working to improve its AML program. Moneytun LLC shall not engage in international, physical transportation of money or monetary instruments.

Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of the USA PATRIOT Act of 2001 and the implementing regulations under it.

~~~~~~~~~~~~~~~~~~~~~~SIGNATURE PAGE FOLLOWS~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~

Reviewed and Approved by:

ARTHUR AVETISIAN /
COMPLIANCE OFFICER

Date: February 10th 2014