CS INV VEN Inc.

dba: FINUS

Anti-Money Laundering & Counter Terrorist Financing

Compliance Program:
Internal Controls, Policies & Procedures

Originally Adopted: October 1, 2023

Policy Statement

This Anti-Money Laundering & Counter Terrorist Financing Program established by CS INV VEN Inc. dba: FINUS (referred to as "FINUS" or "the Company" for the duration of this document) is used to detect and prevent money laundering using the entity known as FINUS as well as stating the policies and procedures to the employees of FINUS.

This includes money laundering for criminal intent as well as terrorist financing.

The Company has integrated its Anti-Money Laundering (AML) & Counter Terrorist Financing (CTF) Compliance Program.

Due to the limited size of the Company, FINUS staff is responsible for the implementation of the AML & CTF policies, procedures, and internal controls.

As an MSB, FINUS has committed to compliance with all applicable state and federal anti-money laundering and counter terrorist financing rules and regulations. This includes compliance with the Bank Secrecy Act, USA Patriot Act, OFAC, & industry best practices for AML & CTF.

FINUS offers its customers the service of money transmission or money remittance and for this reason, an AML & CTF compliance program has been established. This AML & CTF Program has been established and implemented to monitor the Company's transactions and identify any potential AML & CTF risks, reportable transactions, and suspicious activity.

Policy Background

FINUS maintains an AML & CTF Compliance program in accordance with the Bank Secrecy Act, USA Patriot Act**,** and industry best practices related to combatting money laundering and terrorist financing. It is the policy of FINUS to operate an AML & CTF compliance program in accordance with the five (5) pillars of AML compliance.

The USA Patriot Act:

The USA Patriot Act ("Act") was enacted in October 2001 as a measure to combat terrorism. The provisions of the Act deal with a variety of areas, from immigration to money laundering. Below you will find a summary of key provisions of the Act relevant to the money service business, which deal with anti-money laundering and terrorist financing prevention:

The Act requires financial institutions to establish Anti-Money laundering programs, including at a minimum the five (5) pillars of AML Compliance:

- **The development of written internal controls, policies and procedures to comply with Federal Law and Regulations.**
- **The designation of a compliance officer.**
- **An ongoing employee-training program.**
- **An independent review function to test the compliance program**
- **Enhanced customer due diligence.**

31 CFR :

§ 1022.210 Anti-money laundering programs for money services businesses.

(a) Each money services business, as defined by § 1010.100(ff) of this Chapter, shall develop, implement, and maintain an effective anti-money laundering program. An effective anti-money laundering program is one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.

(b) The program shall be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the money services business.

(c) The program shall be in writing, and a money services business shall make copies of the anti-money laundering program available for inspection to the Department of the Treasury upon request.

(d) At a minimum, the program shall:

(1) Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with this chapter.

(i) Policies, procedures, and internal controls developed and implemented under this section shall include provisions for complying with the requirements of this chapter including, to the extent applicable to the money services business, requirements for:

(A) Verifying customer identification;

(B) Filing reports;
(C) Creating and retaining records; and
(D) Responding to law enforcement requests.

(ii) Money services businesses that have automated data processing systems should integrate their compliance procedures with such systems.

(iii) A person that is a money services business solely because it is an agent for another money services business as set forth in § 1022.380(a)(2), and the money services business for which it serves as agent, may by agreement allocate between them responsibility for development of policies, procedures, and internal controls required by this paragraph (d)(1). Each money services business shall remain solely responsible for implementation of the requirements set forth in this section, and nothing in this paragraph (d)(1) relieves any money services business from its obligation to establish and maintain an effective anti-money laundering program.

(2) Designate a person to assure day to day compliance with the program and this chapter. The responsibilities of such person shall include assuring that:

(i) The money services business properly files reports, and creates and retains records, in accordance with applicable requirements of this chapter;

(ii) The compliance program is updated as necessary to reflect current requirements of this chapter, and relate guidance issued by the Department of the Treasury; and

(iii) The money services business provides appropriate training and education in accordance with paragraph (d)(3) of this section.

(3) Provide education and/or training of appropriate personnel concerning their responsibilities under the program, including training in the detection of suspicious transactions to the extent that the money services business is required to report such transactions under this chapter.

(4) Provide for independent review to monitor and maintain an adequate program. The scope and frequency of the review shall be commensurate with the risk of the financial services provided by the money services business. Such review may be conducted by an officer or employee of the money services business so long as the reviewer is not the person designated in paragraph (d)(2) of this section.

(e) *Compliance date.* A money services business must develop and implement an anti-money laundering program that complies with the requirements of this section on or before the later of July 24, 2002, and the end of the 90-day period beginning on the day following the date the business is established

Employee Training Program & Procedures

Initial Training

All employees are required to undergo training upon being hired at FINUS. Initial training is required to be conducted within 30-days of the employees date of hiring.

Employees are provided with a copy of these AML Policies and Procedures as well as training materials focusing on Anti-Money Laundering and Counter Terrorist Financing. Employees are also provided with written documentation created specifically for the recognizing and reporting of suspicious activity relating to financial crimes conducted through money transmissions and money remittances. All employee training is to be documented within employee training logs. Employee training logs are to include the name of the employee trained, the date the employee trained, and the subject of the training matter. FINUS may distribute additional training to its employees. Additional training may require employees of FINUS to undergo testing and complete a quiz or test after training has been conducted. FINUS will securely maintain all training materials and corresponding training documentation for its employees. Additional training materials may include but not be limited to: certificates of training, certificates of attendance for AML seminars, certificates of attendance for AML webinars, employee-completed quizzes, memberships to associations, etc.

Documentation of training is maintained securely by FINUS along with testing of employees upon completion of the training sessions and is not to be shared with any employee who is not considered Senior Management. Results of the employee training are discussed between the Compliance Officer / Senior Management of FINUS and the employee who underwent the training. Any open issues or deficiencies are immediately addressed with the employee.

Employee Training Sessions are to include at a minimum, the following:

- Definitions of Money Laundering
- Definitions of Terrorist Financing
- Definitions of the Bank Secrecy Act (BSA) and the related Compliance Requirements.
- Definitions of the USA Patriot Act and the related Compliance Requirements.
- Rules and Regulations of the Financial Crimes Enforcement Network (FinCEN)
- Rules and laws of the State of Florida.
- Rules and regulations of the Florida Office of Financial Regulation.
- Currency Transaction Reporting (CTR)
- Monitoring of customer transactions and activity
- Identifying unusual or potentially suspicious activity
- Suspicious Activity Reporting (SAR)
- Customer Identification Program and Verification
- Know Your Customer (KYC) Program.
- How to respond to customers who want to circumvent filing requirements or laws.

Ongoing and Refresher Training

The Compliance Officer provides refresher & ongoing training to all employees.

- Refresher & ongoing training is immediately provided based upon any new regulatory requirements, policies and procedures or changes of policies and procedures issued by any governmental agency or regulatory agency.
- Refresher & ongoing training is immediately provided based upon any changes in any laws, or updates, directly affecting the business, specifically the Bank Secrecy Act and the USA Patriot Act.
- Refresher & ongoing training is immediately provided based upon any new requirements, policies and procedures or changes of policies and procedures issued by any third parties or vendors of the Company.
- Refresher Training and ongoing training is to be conducted on a periodic basis, commensurate with the risks of the Company
- All refresher & ongoing training is to be documented at a minimum within the Company's employee training logs.
- Additional refresher training may be documented within certificates of training, employee-completed quizzes, and membership certifications to third party organizations.
- The Compliance Officer reviews all compliance exceptions found with employees and provide immediate retraining and refresher training. This information is documented by the Compliance Officer
- Refresher training is provided upon review from the Compliance Officer if it is determined that an employee requires refresher training based upon performance.
- Refresher training and ongoing training will be distributed no later than 4 months from the date of the employees initial training
- Refresher training and ongoing training is performed on an annual basis at the minimum.

Compliance Officer Training

The Compliance Officer of FINUS is required to undergo training. It is the policy of the Company that all compliance officer training be documented. Training documentation can include but not be limited to: certificates of training, certificates of membership in third party organizations, completed quizzes & tests, and employee training logs.

The Compliance Officer reviews any and all bulletins, notices and updates issued by governmental agencies, regulatory agencies and vendors. The Compliance Officer may receive training from third party organizations focusing on AML and CTF. Training can be conducted via in person seminar or online webinars.

All training documentation is to be maintained for 5-years from the date of training.

Designation of a Compliance Officer

In accordance with the Bank Secrecy Act and USA Patriot Act of 2001 as well as industry best practices, FINUS has designated a Compliance Officer.

The written designation of the Compliance Officer is memorialized in a separate and distinct document with the approval of the Company.

The Compliance Officer is designated by the Senior Management of FINUS. The designation must be documented and approved by senior management. The Compliance Officer is authorized to, and reports directly to the Senior Management of FINUS.

The Compliance Officer is the primary point of contact for all internal and external questions relating to money laundering and terrorist financing matters and the policy requirements described within this document. The duties of the Compliance Officer include but are not limited to:

- Implementing FINUS' AML & CTF Compliance Program at the operational level.
- Reviewing and updating the AML and CTF Compliance Program consistent with any new statutes, regulations, industry best practices, or changing products or product features.
- Overseeing AML and CTF communication and training for personnel. Distributing all AML & CTF training to employees, and securely maintaining that corresponding training documentation.
- Ensuring reporting and recordkeeping is in accordance with the requirements of the BSA and USA Patriot Act. This includes ensuring that all potential CTRs and SARs are filed when activity subject to filing requirement occurs.
- Coordinating independent reviews of FINUS' AML & CTF Compliance Program.
- Ensuring that a Customer Identification Program (CIP) and Know Your Customer (KYC) Program is properly implemented by FINUS. This includes implementing the fifth pillar of AML Compliance, Customer Due Diligence, which requires identifying the beneficial ownership of any FINUS customer.

Pursuant to 31 CRF §1022.210(d)(2):

Designate a person to assure day-to-day compliance with the program and this chapter. The responsibilities of such person shall include assuring that:

(i) The money services business properly files reports, and creates and retains records, in accordance with applicable requirements of this chapter;
(ii) The compliance program is updated as necessary to reflect current requirements of this chapter, and relate guidance issued by the Department of the Treasury; and
(iii) The money services business provides appropriate training and education in accordance with paragraph (d)(3) of this section.

Compliance Officer's Duties and Responsibilities

Policies and Procedures

- Maintains a documented AML Program which is customized specifically for FINUS. Ensure that written internal controls, policies, and procedures are implementable.
- Reviews the Company's operations to ensure that they are performed in accordance with FINUS' documented AML procedures.
- Stays up to date on all upcoming federal and state rules and regulations. Updates the Company's AML Program to include any upcoming applicable rules and regulations.

Training

- Ensures that all employees receive their initial training within 30-days of being hired.
- Ensures that all employees undergo refresher training on an at least annual basis.
- Maintains all resulting employee training documentation securely.

Monitoring

- Reviews each CTR filed for accuracy and completeness prior to filing
- Reviews each SAR filed for accuracy and completeness prior to filing
- Reviews all transactions subject to compliance with the Travel Rule.
- Reviews daily activity report each day for any unusual activity or transaction patterns.
- Reviews transactions each day to ensure that proper customer identification was collected and maintained.
- Reviews transactions performed by employees to monitor for inconsistencies and any potential AML or CTF violations.

Recordkeeping

- Maintains AML & CTF Policies and Procedures.
- Maintain record retention program and requirements.
- Maintain separate and distinct records for transactions subject to reporting requirements.

Documentation

- Reviews all materials related to AML Program.
- Responsible for notifying all staff and employees to any changes in AML program.

Compliance Monitoring

The Compliance Officer's responsibilities include a constant and periodic monitoring of customer activity through FINUS' implemented internal controls, policies and procedures. FINUS will conduct compliance monitoring through a manual review process. The Compliance Officer is to review customer activity on an ongoing and constant basis to identify any activity that requires the filing of a SAR, CTR, or compliance with the Travel Rule.

The following are specific monitoring activities:

- The Compliance Officer reviews transactions to ensure the proper customer identification has been collected and maintained.
- Transactions are reviewed to determine any unusual transaction patterns or any potential suspicious activity.
- Customer files are reviewed periodically to determine if questionnaire answers correspond to the activity conducted by the customer
- Review of customer transactions against the expected transaction activity stated by the customer at the outset of the relationship. Review to ensure that the customer has represented themselves accurately
- Systematic review by Compliance Officer for transactions performed by employees which are subject to reporting requirements but were not properly reported.
- Review of employee paperwork and documentation on transactions performed by employees.
- Compliance Officer reviews transactions on a daily basis to determine if activity is subject to regulatory reporting requirements or enhanced due diligence.
- Compliance Officer reviews transactions on a weekly basis to determine if activity has been structured to avoid the filing of a CTR or compliance with the Travel Rule.

AML Policies and Procedure

It is the policy of FINUS to maintain documented Internal Controls, Policies and Procedures in accordance with the Bank Secrecy Act and USA Patriot Act. The AML policies and procedures must include the five pillars of AML compliance: Compliance Officer Designation, Employee Training Program, Independent Review, Customer Due Diligence, and Establishment of a documented AML Program.

The AML Policies and Procedure are to be reviewed by senior management on an annual basis. The document requires the senior management approval on an annual basis. All updates, amendments, and changes to the documented program are to be recorded within these AML Policies and Procedures. The document is to be updated for all changes to relevant State and Federal rules regulations and laws.

Independent Review of the AML Compliance Program

It is the policy of the Company to undergo an Independent Review of its AML Compliance Program on a periodic basis commensurate with the risks of FINUS' operations.

The Company retains an outside independent reviewer to perform the Independent Review function of the Anti-Money Laundering Program.

The independent review is to be performed every 12-14 months. The frequency of the independent review is commensurate with the transactional risks posed by the Company.

We require the reviewer to provide a written report, which include the results of the examination and any recommendations to the program. Upon receipt of this written report, the Compliance Officer is responsible for taking immediate remedial actions to respond to the examination findings.

The actions taken by the Compliance Officer are to be documented and maintained by the Company, and held for review during the next examination. The Compliance Officer will require the auditor or examiner to address these specific issues during the next examination and respond to the actions taken and the subsequent results.

The review of the Program will include, but not be limited, to the following:

- evaluating the overall integrity and effectiveness of the AML compliance program;
- evaluating the procedures for BSA reporting and recordkeeping requirements;
- evaluating the implementation and maintenance CIP;
- evaluating the customer due diligence requirements;
- evaluating the transactions, with an emphasis on high-risk areas;
- evaluating the adequacy of the staff training program;
- evaluating the systems, whether automated or manual, for identifying suspicious activity;
- evaluating the system for reporting suspicious activity;
- evaluating the response to previously identified deficiencies;
- Required Registrations ;
- Designation of Compliance Officer;
- Know Your Customer (KYC) & Know Your Employee (KYE) Programs;
- Risk Assessment Applications ;
- Review of Written Internal Controls, Policies & Procedures;
- Employee Training;
- Currency Transaction Reports (CTR's);
- Suspicious Activity Reports (SAR's) ;
- OFAC Program ;
- Gramm-Leach-Bliley Act Compliance.

Know Your Customer and Customer Identification Program

FINUS is committed to preventing the use of its products by persons who seek to launder the proceeds of criminal activity, finance terrorism, or conduct other criminal acts. Risk of abuse is presented in large part through customers. Therefore, the Company has adopted a Customer Identification Program (CIP) to assist in managing its AML & CTF risk. It is policy to conduct full CIP on all customers, including both retail (individuals) and commercial (legal entities) customers.

FINUS' CIP is a critical component of the AML & CTF Program. CIP embodies the concept that, in order to identify what is unusual activity for a customer, one must have established a sufficient understanding of what is usual and expected activity, consistent with the purpose and intended usage of the account relationship. Activity that is outside the norm or inconsistent with an institution's understanding may be suspicious and require reporting to federal authorities.

FINUS' CIP includes: (i) basic policies and procedures for collecting and verifying information on the identity of customers; (ii) enhanced policies and procedures for gathering further information about customers to gain a better understanding of the relationship and anticipated transaction activity; and (iii) policies and procedures for monitoring customer activity throughout the life of the relationship.

FINUS has established a Know Your Customer (KYC) program to familiarize itself with its customers transactions and transaction patterns. FINUS KYC program is established through the monitoring the onboarding of customers and monitoring the transactions customers conduct. The Compliance Officer of FINUS is to gain a familiarity and understanding of the transactions being conducted by its customers. This may include but not be limited to the Compliance Officer understanding why a customer is conducting a transaction, why the customer conducts a transaction of a certain volume, why a customer conducts transactions at a certain frequency, and the source of funds from which this customers transaction originates. Implementing a KYC program and understanding customer's reasons for conducting activity, assists FINUS in determining if transactions are unusual or potentially suspicious and requiring a SAR.

The following elements are included in the Company's KYC Program:

- Customer Identification.
- Documenting any issues during the onboarding of a customer
    - Has the customer submitted any false or misleading information
    - Has the customer submitted any false or misleading documentation
    - Has the customer attempted to create an account with FINUS multiple times
    - Was the customer rejected during the initial onboarding process

- Assessment of risk related to customer transactions.
    - Why is the customer conducting the transaction

    - Why is the customer conducting transactions of such a high volume
    - Why is the customer conducting transactions at such a high frequency
- Definition and acceptance of customer identification in context of the services offered
- Customer account and transaction monitoring based upon risks presented.
    - Is this a high risk activity
    - Is the customer conducting a transaction from a high risk country
- Investigation and examination of unusual customer activity.
- Documentation of findings.
- Appropriate internal and external reporting.
- Reviewing KYC system.
- Staff training.

Employees are trained to recognize repetitive transactions or repeat customer transactions, i.e. daily transactions, weekly transactions, monthly transactions, transactions of the same volume being conducted, patterns of transactions, deviation of a customer's transaction pattern, volume, or frequency.;. This information is used to develop a "Know Your Customer" program. The Compliance Officer is responsible to recognize and identify customer patterns and usage to detect suspicious activity.

Customer Identification Program & Requirements

All FINUS customers are required to be identified through the Company's CIP. It is the policy of FINUS not to conduct transactions with any individual or company that cannot be properly identified or verified. FINUS requires all customers to be properly identified and to have their identity verified. FINUS will not conduct transactions with any individual or legal entity in which the Company believes are misrepresenting their identity.

It is the policy of FINUS to conduct its customer identification program using a non-documentary verification process. FINUS will collect its customers information and verify this information through a third-party non documentary verification source. FINUS relies on information received from its customers to be truthful and transparent. If FINUS believes any information received to be false or non-transparent, the company reserves the right to decline the customers application during the onboarding process.

To conduct its non-documentary verification of its customer identity, FINUS requires the following to be submitted from every customer:

Individuals:

- Individual's Legal Name
- Individual's Legal Address
- Individual's Date of Birth
- Social Security Number (SSN / SS#)

The Company collects the abovementioned information in order to properly verify the identity of its customers. FINUS collects the abovementioned information in order to properly verify that the individual is who they say they are.

The abovementioned information is collected by FINUS and entered into a non-documentary verification solution offered through a third-party company. Information is scrubbed against open source databases to verify the identity of the individual. If the third-party solution results in the identity of the customer being fully verified, FINUS reviews these results and determines whether the customer is to be onboarded. If the third-party solution cannot fully verify the identity of the customer, the customers application and onboarding process will fall to a documentary verification process.

Customers who fail the non-documentary verification process, will be allowed to apply through a documentary verification process, at the discretion of FINUS' Compliance Officer. FINUS requires all customers attempting to be onboarded through documentary verification to submit two (2) separate forms of documentation. The first form of documentation required is a government-issued photo ID. Government issue-ID can include any of the following:

- U.S. Driver's License
- U.S. Residence Card
- U.S. or Foreign Passport with a valid J-551 Stamp
- Welfare/Medicaid card with Photo
- U.S. State Firearms Permit with Photo
- U.S. State-Issued Identification Card
- U.S. Military Identification Card
- Mexican Matricula Consular Card
- U.S. Issued Permanent Resident Card (Green Card)
- Guatemalan Consular Card (UTB only)
- U.S. Employment Authorization Card (RBC only)

The abovementioned photo ID, must be accompanied by a secondary document which states the legal address of the customer. The address on the first document must match the address on the secondary document. If the addresses do not match, FINUS will not onboard the customer. Secondary documentation includes the following:

- Utility Bill Statement (must include a date within the prior 3-months)
- Credit Card Statement (must include a date within the prior 3-months)
- Lease Agreement
- Mortgage Statement

- Insurance Policy or Statement

The Compliance Officer of FINUS will review the two forms of identification and determine whether the individual's identity can be verified. If the Compliance Officer believes the individuals identity cannot be verified, the customer will not be onboarded and will be prohibited from conducting transactions with FINUS. If the Compliance Officer believes the individuals identity to be verified, the customer will move to the final stage of the onboarding process.

OFAC Verification Prior to Onboarding

In compliance with the BSA and USA Patriot Act, FINUS does not conduct transactions with any individual listed on OFAC's Specially Designated Nationals (SDN) & Blocked Persons List. Once an individual's identity has been verified, FINUS will conduct a search of that individual to the most recently updated SDN & Blocked Persons List issued by the OFAC & the US Treasury Department. FINUS conducts a manual search of the individual to OFAC's SDN List using a third-party search engine. This search is to be conducted through the U.S. Department of Treasury's Sanctions List Search tool (Sanctionssearch.ofac.treas.gov) or a similar search engine such as www.InstantOFAC.Com.

If the search of the individual to these sanctions databases results in no match, no hit, or no findings, FINUS will onboard the customer and permit them to conduct transactions.

If the search of the individual to these sanctions databases results in a direct match, positive hit, or partial findings, FINUS will not onboard the customer and prohibit the individual from conducting transactions through the Company.

To conduct verification of its customers identity for its legal entity customers, FINUS requires the following information and documentation to be submitted from each customer:

Legal Entities:

- Legal Name of the Company
- Legal Address of the Company
- The State in which the Company was formed/ organized
- List of all individuals / entities who own 25% or more of the Company
    - Include Names & Ownership Percentage
- The name of the authorized individual submitting the Company's application
- The legal address of the authorized individual submitting the Company's application

- The date of birth of the authorized individual submitting the Company's application

- Entity Formation Documentation (which can include any of the below)
    - Articles of Incorporation
    - Articles of Organization
    - Minutes of Organization
    - Corporate Bylaws
    - Operating Agreements
    - Board Resolutions

The Company collects the abovementioned information and documentation in order to properly verify the identity of its customers (both the legal entity, as well as the individual representing the legal entity). The Company ensures that any individual representing the Company is who they say they are, and validates both the entity and individuals information.

FINUS will first verify the identity of the individual representing the Company by conducting the same non-documentary verification process as written earlier in this document. If non-documentary verification fails, then documentary verification will be performed on the individual, as stated earlier in this document.
If the individual representing the Company is able to be verified by FINUS, then the legal entity's customer onboarding process will move on to the next stage. Using a third-party solution for verifying the identity of legal businesses, FINUS will conduct a Know Your Business (KYB) verification process. FINUS will use the information submitted for the legal entity (legal name, legal address, State in which the Company was organized / formed) and scrub this information against an open source solution provided by a third-party company. FINUS will compare the results of this non-documentary verification process against the formation documentation submitted, to ensure that the information obtained through non-documentary verification corresponds to the documentation submitted by the customer.

In addition to verifying the identity of the legal entity, FINUS conducts an independent search of entity to the appropriate State database in which the entity is registered. FINUS will conduct a manual search of the Legal Entity's name to the Secretary of State or applicable State website in which the legal entity was organized, incorporated, or formed. *For example, a New York company would be searched against the New York Department of State, Division of Corporations website.*

OFAC Verification Prior to Onboarding

In compliance with the BSA and USA Patriot Act, FINUS does not conduct transactions with any individual nor entity listed on OFAC's Specially Designated Nationals (SDN) & Blocked Persons List. Once an individual's identity and entities identity has been verified, FINUS will conduct a search of the individuals and the entity to the most recently updated SDN & Blocked Persons List issued by the OFAC & the US Treasury Department. FINUS conducts a manual search of the individuals and entity to OFAC's SDN List using a third-party search engine. This search is to be conducted through the U.S. Department of Treasury's Sanctions List Search tool (Sanctionssearch.ofac.treas.gov) or a similar search engine such as www.InstantOFAC.Com. In addition to the authorized individual and the legal entity being searched against OFAC, FINUS will conduct a search of all beneficial ownership to OFAC using the same process.

If the search of the individuals or entity to these sanctions databases results in no match, no hit, or no findings, FINUS will onboard the customer and permit them to conduct transactions.

If the search of the individuals or entity to these sanctions databases results in a direct match, positive hit, or partial findings, FINUS will not onboard the customer and prohibit the individual from conducting transactions through the Company.

The Customer Due Diligence Rule

It is the policy of FINUS to onboard all customers in accordance with the fifth pillar of AML compliance, the Customer Due Diligence Rule. The CDD Rule states that the Company must:

- **Identify and verify the identity of customers**
- **Identify and verify the identity of the beneficial owners of companies opening accounts. Financial institutions will have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity, and an individual who controls the legal entity.**
- **Understand the nature and purpose of customer relationships to develop customer risk profiles**
- **Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information**

It is the policy of FINUS to request that all legal entity customers provide a transparent view of its ownership structure which includes all beneficial ownership. FINUS requires these customers to provide the full legal name of any individual who owns 25% or more of the legal entity. If a customer is unwilling or unable to provide its beneficial ownership structure to FINUS, FINUS will not onboard the customer.

Customer Identification: It is the Policy of the Company to Comply with 31 CFR §1010.12 Identification Required.

Before concluding any transaction with respect to which a report is required under § 1010.311, § 1010.313, § 1020.315, § 1021.311 or § 1021.313 of this chapter, a financial institution shall verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and the social security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States must be made by passport, alien identification card, or other official document evidencing nationality or residence (*e.g.*, a Provincial driver's license with indication of home address). Verification of identity in any other case shall be made by examination of a document, other than a bank signature card, that is normally acceptable within the banking community as a means of identification when cashing checks for nondepositors (*e.g.*, a driver's license or credit card). A bank signature card may be relied upon only if it was issued after documents establishing the identity of the individual were examined and notation of the specific information was made on the signature card. In each instance, the specific identifying information (*i.e.*, the account number of the credit card, the driver's license number, *etc.*) used in verifying the identity of the customer shall be recorded on the report, and the mere notation of ''known customer'' or ''bank signature card on file'' on the report is prohibited.

It is the policy of the Company to maintain all customer identification and all customer information for a period of 5-years. All information and identification is to be maintained for 5-years from the date of the customers last transaction.

Gramm-Leach-Bliley Act

Privacy Provisions

FINUS is required to comply and adopt a policy in accordance with The Gramm-Leach-Bliley Act, to prevent unauthorized disclosures of all personal non-public information the Company receives from its customers.

Accordingly, it is the policy of FINUS to protect the privacy of all personal, non-public information provided by its customers. FINUS shares no information provided by its customers other than allowed by applicable laws. If customer information is to be shared with any party outside of FINUS' organization, a valid written legal request must be received.

It is FINUS' policy to safeguard all customer data from theft or improper sharing. This includes, but is not limited to, all collected customer information and transactional data.
In order to ensure compliance, the Compliance Officer shall oversee system access requests, terminating access after departure of an employee and contractor, and ensuring employees only have access to the data required to carry out their duties.
All employee workstations must have sufficient firewalls and virus protection to ensure data is not inadvertently shared. Additionally, all employees and individuals with access to customer data will undergo annual information security training.
FINUS will ensure that all third-party vendors, with whom data is shared, have sufficient data controls in place to comply with GLBA.

Accordingly, it is the policy of FINUS to protect the privacy of all personal, non-public information provided by its customers. The Company shares no information provided by its customers other than allowed by applicable laws. In addition the Company had adopted the following policies in accordance with privacy provisions:

- The Company does not leave customer information and records in areas that are accessible by non-employees.

- The Company does not dispose of records with private customer information, in a manner that makes those records accessible to the public.

- The Company has established passwords and other protections to ensure that electronic records are not accessible to the public.

- Senior Management is advised within 24 hours of any unauthorized disclosure of customer information.

Consumer Financial Protection & Privacy Policies:

- Before FINUS collects personally identifiable information ("PII") FINUS tells its customer what information is being collected, why the Company is collecting it, and how the Company is going to use it. FINUS only collects the minimum amount of PII necessary to achieve the task, which is appropriately verifying the identity of its customers. FINUS works to ensure that the PII collected and maintained by the Company is relevant, timely, and complete. It is the policy of FINUS to properly store and maintain all PII and all employees are trained to ensure that PII remains protected. FINUS takes consumer privacy very seriously and will never share consumer information with other customers. Consumer information will never be shared with third parties unless legal requests such as subpoenas are received.

§1016.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§1016.13, 1016.14, and 1016.15.

(b) *Scope.* (1) This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to those financial institutions and other persons for which the Bureau of Consumer Financial Protection (Bureau) has rulemaking authority pursuant to section 504(a)(1)(A) of the Gramm-Leach-Bliley Act (GLB Act) (15 U.S.C. 6804(a)(1)(A)). Specifically, this part applies to any financial institution and other covered person or service provider that is subject to Subtitle A of Title V of the GLB Act, including third parties that are not financial institutions but that receive nonpublic personal information from financial institutions with whom they are not affiliated. This part does not apply to certain motor vehicle dealers described in 12 U.S.C. 5519 or to entities for which the Securities and Exchange Commission or the Commodity Futures Trading Commission has rulemaking authority pursuant to sections 504(a)(1)(A)-(B) of the GLB Act (15 U.S.C. 6804(a)(1)(A)-(B)). Except as otherwise specifically provided herein, entities to which this part applies are referred to in this part as "you."

(2)(i) Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-1320d-8).

(ii) Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution described in §1016.3(l)(3) of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

(3) Nothing in this part shall apply to:

(i) A financial institution that is a person described in section 1029(a) of the Consumer Financial Protection Act of 2010, title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), Public Law 111-203, 124 Stat. 1376 (12 U.S.C. 5519(a));

(ii) A financial institution or other person subject to the jurisdiction on the Commodity Futures Trading Commission under 7 U.S.C. 7b-2;

(iii) A broker or dealer that is registered under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.;*)

(iv) A registered investment adviser, properly registered by or on behalf of either the Securities Exchange Commission or any state, with respect to its investment advisory activities and its activities incidental to those investment advisory activities;

(v) An investment company that is registered under the Investment Company Act of 1940 (15 U.S.C. 80a-1 *et seq.;*) or

(vi) An insurance company, with respect to its insurance activities and its activities incidental to those insurance activities, that is subject to supervision by a state insurance regulator

Know Your Employee (KYE)

An important part of any Compliance Program is understanding and gaining insight into the employees, as well as detecting any potential employee problems, using the program.

- All employees handling MSB transactions or conducting AML & CTF related responsibilities, must be monitored by the Compliance Officer.
- The Compliance Officer must review the resume of any abovementioned employees to identify any previous experience working with MSBs, AML, or CTF related industries.
- Employee reviews and evaluations may be conducted by the Compliance Officer and then reported to the Senior Management of the Company
- All employees must be searched to the OFAC database prior to being hired by FINUS and conducting any transactions or operations.
- Random testing of employee transactions may be conducted by the Compliance Officer, if believed to be necessary.
- Compliance Officer may discuss any employee issues or deficiencies noticed with the Senior Management and corrective actions may be taken.

Employee & Employment Procedures

- All employees are subject to background checks. The Compliance Officer or designee reviews the background check. The background check may be expanded to include a credit/judgment check search provided the applicant gives written consent. In the case that an applicant is considered high risk, at Management's discretion, the applicant will be denied employment. All employees are subject to being searched against Sanctions lists prior to hiring. Employees may be subject to being searched against Sanctions lists at any time during their employment. If an employee is found to be a direct hit or positive match to sanctions lists, the employee may be immediately terminated.

- All employee applications are reviewed independently by the Compliance Officer In the case that an applicant has prior work experience in a money transmitter, money remitter, licensed check casher, or foreign currency exchange, management carefully evaluates the applicant's training, experience and previous job performance. The Compliance Officer or the Senior Management of FINUS assesses the applicant's training and provide the necessary training to bring the applicant up to the standards of the FINUS: Anti-Money Laundering & Counter Terrorist Financing Compliance Program.

- Appropriate forms of identification are reviewed, and then photocopied and maintained in the employees file along with a copy of the employment application. The Compliance Officer examines all identification provided by applicants. All identification presented by the employee or applicant must be an acceptable form of identification. Acceptable forms of identification include a

photo driver's license, passport, resident alien card, social security card, or other valid government issued identification. The Compliance Officer may request additional identification, which is subject to independent verification.

- Employee files have limited access and are maintained in a secure area. Employee files are only accessible to approved personnel determined by FINUS' Senior Management.

- All employees are subject to a 60-day probation period. This period may vary and is at the sole discretion of Senior Management. Factors that affect the probationary period would include, but not be limited to, the employee's previous work experience as well as employee's skills and abilities. Without exception, all new employees require supervisory approval when conducting transactions until the employee is well versed and has become familiar with the customers and the Company's policies and procedures.

OFAC & Sanctions Review Program

a) As an entity subject to rules and regulations from FinCEN, FINUS is prohibited from engaging in transactions involving: (I) countries which are considered hostile to the U.S or under some type of U.S. embargo or sanction; and/or (II) specially designated nationals (hereinafter referred to as "SDN's"), terrorists, and narcotics traffickers (hereinafter referred to as "Blocked Persons").

b) The Office of Foreign Assets Control ("OFAC") administers the various laws that prohibit the conduct of business with hostile nations and Blocked Persons. Severe civil and criminal penalties exist for violations of these laws.

c) OFAC makes public the embargoed nations and alphabetical master lists of Blocked Persons ("OFAC lists"). The OFAC lists are amended from time to time and are available in OFAC's website at http://www.treas.gov/offices/enforcement/ofac/.

Financial institutions are required to block transactions they accept, which involve an embargoed nation or a Blocked Person. The institution must report the transaction to OFAC and block the corresponding funds until receipt of instructions from OFAC. Usually prior to releasing a transaction, the Company will need to obtain additional customer information to assist in the evaluation process.

If a customer appears as a hit on the OFAC list it is the policy of the Company to review the transaction to determine if in fact they are the SDN or if the customer is not the SDN but has the same name.

Initial & Ongoing OFAC Checks

All customers conducting transactions are searched against the OFAC database & Sanctions Lists. FINUS searches all individuals and entities against OFAC prior to the individual or entity being onboarded and becoming a customer of FINUS. OFAC searches are conducted on individuals conducting transactions for themselves, legal entities on whose behalf transactions are conducted, individuals conducting transactions on behalf of legal entities, and individuals with beneficial ownership in a legal entity customer of FINUS. All initial OFAC searches are documented and maintained securely by FINUS. The OFAC searches are maintained in the appropriate customer file alongside the information and documentation provided by the customer.

Investigating OFAC Hits

If the OFAC search returns results other than "No Findings", "No Matches", or "No Hits", it is considered a potential OFAC hit. All potential OFAC hits are reviewed by the Compliance Officer and recorded on the OFAC log. If there is an potential hit to the OFAC database, the Company will review the Customers' information to the Potential OFAC Hit's information. The Company will review secondary identification factors such as Date of Birth or Country of Origin which are provided on OFAC search results to that of FINUS' customer. If the customer has the same date of birth and country of origin as

the individual on the OFAC list, this is a match and the customer will not be permitted to conduct transactions. If the customers date of birth and country of origin are different from the Individual on the OFAC database, this is an indirect hit or partial match. The Company will print the search result documentation and maintain in a separate OFAC folder. Any hits that cannot be cleared or validated are reported to OFAC for further instructions.

Reporting OFAC Matches

If an OFAC match is confirmed, the Compliance Officer has 10 calendar days to report the hit to OFAC. The customer's account is permanently suspended in the event of a validated OFAC match.

Blocking Funds

If an OFAC match is confirmed on a transaction, any funds in the accounts held by FINUS is blocked according to OFAC requirements. Blocking and freezing of funds is the responsibility of FINUS

Recordkeeping

An OFAC log is maintained to show results of all cleared or validated hits reviewed. Log is maintained by the Compliance Department and is kept for five (5) years after the date of the hit. In addition, any reports made to OFAC are maintained for five (5) years after the date of report.

Prohibited Countries

In addition to prohibited transactions or accounts for persons on the OFAC SDN lists, FINUS restricts transactions in OFAC sanctioned countries. FINUS conducts transactions with customers located in countries outside of the United States. For international transactions, the Company is required to perform enhanced due diligence to ensure that the customer is not operating out of an OFAC sanctioned country. If a customer is identified as being from an OFAC sanctioned or prohibited country, the transaction will not be permitted to occur.

Risk Assessment & Risk Based Approach

It is the policy of FINUS to establish the potential money laundering risks and terrorist financing risks using a risk assessment or a risk based approach towards conducting and monitoring transactions.

This risk assessment is the identification and analysis of relevant risks to the achievement of the Company's objectives, for the purpose of determining how those risks should be managed.

A proper AML & CTF risk assessment measures the company's AML & CTF risk based on its customer, its services, its transaction volumes & frequencies, and the geographic risks it faces. No two companies' risk assessments will be alike. Conducting a thorough AML & CTF Risk Assessment is crucial to building a risk-based approach to BSA/AML compliance.

It is FINUS' policy to conduct an AML & CTF Risk Assessment on an annual basis, or more often if changes in business lines (services, customers, procedural changes) warrant. The Risk Assessment is to be conducted by the Compliance Officer and provided to the Senior Management of FINUS for review and approval. The Risk Assessment is to be reviewed by the Senior Management of FINUS annually as part of their review and approval of the Company's overall AML & CTF Compliance Program.

Each customer is risk rated through a non-documentary process in order to assess applicable risks and implement appropriate controls. Although the risk of each customer or transaction is not documented, FINUS conducts and monitors transactions using a risk based approach. The following factors are considered when reviewing customer transactions and FINUS' procedures:

- How often are customers conducting transactions
- Is the customer conducting transactions at a greater frequency than anticipated
- What is the total monetary value of transactions conducted by the customer
- Is the customer conducing transactions at a higher volume than anticipated
- Is the customer conducting transactions from a high-risk area
- Is the customer conducting transactions just below reportable thresholds
- Are FINUS' systems being properly implemented to mitigate money laundering and terrorist financing risks
- Are there risk mitigating controls that can be implemented by FINUS

Registration & Licensing Requirements

FINUS is registered as a Money Service Business (MSB) as prescribed by the Internal Revenue Service, Department of Treasury, under Section 31 CFR §1022.380, FI

Registration requirement—(1) *In general.* Except as provided in paragraph (a)(2) of this section, relating to agents, each money services business (whether or not licensed as a money services business by any State) must register with the Department of the Treasury and, as part of that registration, maintain a list of its agents as required by 31 U.S.C. 5330 and this section. This section does not apply to the U.S. Postal Service, to agencies of the United States, of any State, or of any political subdivision of a State, or to a person to the extent that the person is an issuer, seller, or redeemer of stored value.
(b) *Registration procedures*—(1) *In general.* (i) A money services business must be registered by filing such form as FinCEN may specify with the Enterprise Computing Center in Detroit of the Internal Revenue Service (or such other location as the form may specify). The information required by 31 U.S.C. 5330(b) and any other information required by the form must be reported in the manner and to the extent required by the form. (ii) A branch office of a money services business is not required to file its own registration form. A money services business must, however, report information about its branch locations or offices as provided by the instructions to the registration form. (iii) A money services business must retain a copy of any registration form filed under this section and any registration number that may be assigned to the business at a location in the United States and for the period specified in § 1010.430(d) of this Chapter.

Although not explicitly required to be registered as an MSB, FINUS has registered as an MSB to reflect its commitment to AML & CTF compliance in accordance with the Bank Secrecy Act and USA Patriot Act.

In accordance with MSB Registration Requirements:

- Renewal of the Company's MSB Registration with FinCEN is required every two calendar years after initial registration.
- FINUS will renew its MSB Registration prior to the expiration of its current MSB Registration.
- A copy of FINUS' current MSB Registration is digitally maintained by FINUS.
- FINUS maintains a copy of its previous MSB Registrations for a five-year period.

Recordkeeping

- All transactional records are maintained in a secure area, by the Compliance Officer.
- All customer identification records are maintained in a secure area by the Compliance Officer.
- Access to records is limited to Compliance Officer and Senior Management, and any individual designated by the Compliance Officer or Senior Management.
- All copies of records, (Customer Files, CTRs, SARs) are maintained in duplicate, with both an original and a backup copy.
- All backup information for Customer Files, CTRs, and SARs are maintained in office and kept for a period of five years.
- Files and documents are maintained in date order and filed by office staff.
- Separate and distinct files are maintained for Customer Transactions, Customer Identification, and CTRs and SARs filed by the Company.
- Separate files are maintained for any information received from governmental agencies, regulatory agencies as well as vendors.

Document Retention

- CTRs are maintained five (5) years from date of filing.
- SARs are maintained five (5) years from date of filing.
- All transactions conducted in excess of $2,999.99 are maintained in compliance with the Travel Rule. For transactions subject to Travel Rule compliance, FINUS will retain corresponding customer identification and the transactional information.
- Transactions subject to compliance with the Travel Rule are maintained five (5) years from the date of the transaction.
- Customer Files and all customer identification are maintained five (5) years from the date of the customers last transaction with the Company. This includes any documentary identification and any non-documentary identification such as information provide by third party CIP solutions.
- Documents, legal requests and any correspondence received or sent to any governmental agency are retained three (3) years from date of receipt.
- Independent Review Reports are maintained for five (5) years from the date of the reports publishing date.
- Any outside or external examinations or audits are maintained for five (5) years from the date of the examination or audit.
- Employee training documentation is maintained for a period of no less than five (5) years.

Travel Rule Requirements- Funds Transfer Rule

Bank Secrecy Act (BSA) rule [31 CFR 103.33(g)]—often called the "Travel" rule—requires all financial institutions to pass on certain information to the next financial institution, in certain funds transmittals involving more than one financial institution.

All transmitter's financial institutions must include and send the following in the transmittal order: The name of the transmitter, The account number of the transmitter, if used, The address of the transmitter, The identity of the transmitter's financial institution, The amount of the transmittal order, The execution date of the transmittal order, and The identity of the recipient's financial institution; and, if received: The name of the recipient, The address of the recipient, The account number of the recipient, and Any other specific identifier of the recipient.

- In compliance with the Travel Rule Requirements, a record of all money transmissions or money remittances and corresponding customer identification is to be maintained for transactions in amounts greater than $3,000 and less than $10,000, fee inclusive. This includes a single transaction or multiple transactions conducted in a 1-day period by a single person or on behalf of a single person.

- Transactions subject to compliance with Travel Rule Requirements are readily available for inspection and may be requested by governmental and regulatory examiners and independent auditors.

- Transactions greater than $10,000 are required to be reported on a CTR.

- The following must be maintained for transactions subject to compliance with Travel Rule Requirements:
    - Customer name, address, Social Security number, date of birth
    - Customer Identification
    - Date of Transaction
    - Dollar amount of Transaction .
    - Type of transaction

Currency Transaction Reports (CTRs)

Although FINUS's current business model does not allow for transactions to be conducted which require the filing of a CTR; FINUS maintains policies and procedures for filing a CTR if the business model were to change.

- CTR's or FinCEN Form 104 are filed for any cash transaction in excess of $10,000.
- Multiple transactions or aggregate transactions must be treated as a single transaction if the entity has knowledge that (I) they are on behalf of the same person, and (II) they result in either currency received (Cash In) or currency disbursed (Cash Out) by the entity totaling more than 10,000 during any one calendar day.
- If structuring of a transaction is suspected, the customer is questioned as to the number, nature, and dollar amount of the transaction performed on that business day.
- Currency is defined as coin or paper money of the United States or any other Country and includes the Euro.
- A currency transaction is any transaction involving the physical transfer of currency from one person to another.
- CTR's must be complete and accurate. All required customer information should be obtained from the customer before the transaction is completed. If information is not available the transaction should not be completed.
- Compliance Officer must review the CTR for completeness and accuracy.
- CTR's are filed no later than 15 days after the completed transaction through FinCEN's BSA E-Filing System. This is the responsibility of the Compliance Officer.
- If contacted by any governmental agency regarding CTR's all information is to be provided immediately to and from the Compliance Officer.
- All CTR's must be filed electronically through FinCEN's Money Service Business E-Filing System.

It is the Policy of the Company that it complies with 31 CFR, regarding the filing of CTR's:

§ 1010.306 Filing of reports.

(a)(1) A report required by § 1010.311 or § 1021.311, shall be filed by the financial institution within 15 days following the day on which the reportable transaction occurred.

(2) A copy of each report filed pursuant to §§ 1010.311, 1010.313, 1020.315, 1021.311 and 1021.313, shall be retained by the financial institution for a period of five years from the date of the report.

(3) All reports required to be filed by §§ 1010.311, 1010.313, 1020.315, 1021.311 and 1021.313, shall be filed with the Commissioner of Internal Revenue, unless otherwise specified.

§ 1010.310 Reports of transactions in currency.

Sections 1010.310 through 1010.314 set forth the rules for the reporting by financial institutions of transactions in currency. Unless otherwise indicated, the transactions in currency reporting requirements in §§ 1010.310 through 1010.314 apply to all financial institutions. Each financial institution should refer to Subpart C of its Chapter X Part for any additional transactions in currency reporting requirements.

§ 1010.311 Filing obligations for reports of transactions in currency.

Each financial institution other than a casino shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000, except as otherwise provided in this section. In the case of the U.S. Postal Service, the obligation contained in the preceding sentence shall not apply to payments or transfers made solely in connection with the purchase of postage or philatelic products.

§ 1010.313 Aggregation.

(b) *Multiple transactions.* In the case of financial institutions other than casinos, for purposes of the transactions in currency reporting requirements in this chapter, multiple currency transactions shall be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than $10,000 during any one business day (or in the case of the U.S. Postal Service, any one day). Deposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit.

§ 1010.314 Structured transactions.

No person shall for the purpose of evading the transactions in currency reporting requirements of this chapter with respect to such transaction:

(a) Cause or attempt to cause a domestic financial institution to fail to file a report required under the transactions in currency reporting requirements of this chapter;

(b) Cause or attempt to cause a domestic financial institution to file a report required under the transactions in currency reporting requirements of this chapter that contains a material omission or misstatement of fact; or

(c) Structure (as that term is defined in § 1010.100(xx)) or assist in structuring, or attempt to structure or assist in structuring, any transaction with one or more domestic financial institutions.

Suspicious Activity Reports (SARs)

All of FINUS' employees must be alert to activity indicative of money laundering, terrorist financing or other criminal activity. It is FINUS' policy to promptly report suspicious activity as required by the BSA and to cooperate with law enforcement in criminal investigations within the confines of applicable federal, state and local laws and regulations.

If an employee of FINUS discovers activity that he or she knows or suspects involves money laundering, terrorist financing or other criminal activity, the information must immediately be referred to the Compliance Officer. The Compliance Officer is required to inform Senior Management when such activity has occurred.

As an MSB, FINUS voluntarily files a "Suspicious Activity Report" with FinCEN if a transaction is conducted or attempted by, at, FINUS, and FINUS knows, suspects or has reason to suspect the transaction or pattern of transactions, FINUS is required to file a SAR for suspicious activity in excess of $2,000 for transactions that:

- Involves funds derived from illegal activity, or is intended to hide or disguise funds or assets derived from illegal activity, as part of a plan to violate or evade any federal law or regulation, or to avoid any transaction reporting requirement under federal law or regulation;

- Is designed, whether by structuring or other means, to evade any requirements of the BSA;

- Serves no apparent lawful purpose, and the reporting MSB knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or

- Involves the use of the MSB to facilitate criminal activity.

It is the policy of FINUS to ensure that all employees handling MSB transactions are properly trained to identify and report suspicious activity to the Compliance Officer for the proper filing of a Suspicious Activity Report (SAR).

Identifying Potential Suspicious Activity

All FINUS employees must be alert to unusual or potentially suspicious activity and transactions not consistent with a customers expected or normal transaction activity.

When establishing new relationships, FINUS staff is required to make reasonable efforts to obtain sufficient information about the customers' business to be able to reasonably anticipate the expected transaction activity. Customer activity is reviewed and monitored on a regular basis to identify activity that may be unusual for the particular customer.

FINUS uses a monitoring system which includes both an automated and manual review of transactions, or patterns of transactions, that may be suspicious. Daily, weekly, and monthly transaction reports are reviewed to identify any unusual or potentially suspicious activity. The Compliance Officer reviews all transaction reports to identify unusual or potentially suspicious activity.

If a transaction, or pattern of transactions, appears unusual or suspicious, regardless of the amount or source of funds, the activity must be referred to the Compliance Officer. It is the responsibility of the Compliance Officer to keep track of internal referrals and to obtain sufficient information concerning the activity to evaluate each referral and make a reasonable determination with respect to the referral. The final decision to report the activity on a Suspicious Activity Report (SAR) shall be made by the Compliance Officer. It is the responsibility of the Compliance Officer to further investigate any internal SAR referral. The Compliance Officer will review the customers transaction history as well as the customers identification to assist in the investigation and reach a conclusion on whether the activity is suspicious and requiring a SAR. If the Compliance Officer believes the activity to be unusual, but not suspicious, then no SAR will be filed. However the Compliance Officer must document its conclusion that the activity is not suspicious. The full suspicious activity investigation must be documented. If the investigation results in the Compliance Officer determining that the activity is indeed "Suspicious", a SAR will be filed.

- The Compliance Officer will download the SAR-MSB form from FinCEN's BSA E-Filing website.
- The Compliance Officer will prepare the SAR and include all available transactional information and customer information that was used in the corresponding suspicious activity.
- All SAR's are to be filed electronically through FinCEN's BSA E-Filing System.
- All SAR documentation is retained for a minimum of five (5) years.

Suspicious activity includes all illegal activity, such as money laundering, structuring of transactions, smurfing, and fraud, which involves the use and movement of funds.

It is the Policy of the Company to comply with the regulations as promulgated under 31 CFR.

§ 1022.320 Reports by money services businesses of suspicious transactions.

(a) *General.* (1) Every money services business, described in § 1010.100(ff) (1),(3), (4), (5), or (6) of this Chapter, shall file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation. Any money services business may also file with the Treasury Department, by using the form specified in paragraph (b)(1) of this section, or otherwise, a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section.

(2) A transaction requires reporting under the terms of this section if it is conducted or attempted by, at, or through a money services business, involves or aggregates funds or other assets of at least $2,000 (except as provided in paragraph (a)(3) of this section), and the money services business knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

(i) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

(ii) Is designed, whether through structuring or other means, to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act; or

(iii) Serves no business or apparent lawful purpose, and the reporting money services business knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

(iv) Involves use of the money services business to facilitate criminal activity.

Identity Theft & Red Flag Detection

Identity theft occurs when an individual or organization steals a customer's personal or financial information and poses as the customer. Identity thieves will attempt to steal information such as social security numbers, medical records, criminal records, residential information and date of birth. This is done with the intention of using the customer's identity to commit fraudulent activities. Fraudsters may pose as a member of a financial institution or family members while attempting to gather this information. Furthermore, these fraudsters will use fake websites and email addresses to gather said personal information.

Identity theft can negatively impact customers in many ways, such as:

- Stealing their funds.
- Committing criminal acts such as fraud under the customer's name.
- Damaging their credit score.

That being said, FINUS works diligently to ensure the safety of its customers' identities and personal identifying information.

FINUS is committed to compliance with the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 and requires an Identity Theft Prevention Policy ("Policy") tailored to the size, complexity and nature FINUS' money transmission and remittance business.

These ID Theft and Red Flag policies enhances FINUS' AML & CTF policy to detect, prevent and mitigate identity theft in connection with the opening of an account or an existing account, and to provide for continued administration of the AML & CTF policy.

Approved by the Compliance Officer, the Red Flag Policy serves to meet the following objectives:

- Identify relevant red flags for the customers or transactions and incorporate those red flags into the monitoring process and fraud detection
- Detect red flags that have been incorporated into this AML policy
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;
- Ensure FINUS' staff are trained as necessary to effectively implement these policies and
- Ensure the policies and procedures are updated periodically to reflect changes in risks to customers and to the safety and soundness of FINUS from identity theft.

FINUS considers the following related to suspicious personal identifying information to be a red flag:

1. Personal identifying information provided is inconsistent when compared against external information sources used for identity verification.
2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources. For example:
    a. The address on the customer's application is the same as the address provided on a previous fraudulent customer application; or
    b. The phone number on a customer application is the same as the number provided on a previous fraudulent customer application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources. For example:
    a. The address on the customer application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid or is associated with a pager or answering service.
5. The Social Security Number provided is the same as that submitted by other individuals attempting to open an account with FINUS.
6. The address or telephone number provided is the same as or similar to the information submitted by another customer attempting to open an account with FINUS.
7. The person attempting to open the account with the FINUS fails to provide all required personal identifying information
8. The personal identifying information provided is not consistent with other personal identifying information that is on file at FINUS.

In order to detect any of the red flags identified above, FINUS maintains a strong CIP & KYC program which includes verifying the identity of all FINUS customers. and persons opening an account on behalf of a legal entity. All customers must pass through FINUS' CIP to be onboarded and conduct transactions.

If any of the abovementioned red flags are identified during the onboarding process, the Compliance Officer will investigate. FINUS will not onboard any customer for which a red flag has been identified, unless a documented investigation is conducted and the red flag proved to be a false positive.

Responding to Legal Process and Other Official Requests

It is not uncommon for MSB's to be served with legal process and requests or receive other written or verbal requests for information from law enforcement and other government authorities in their normal course of business. MSBs routinely receive subpoenas for activity conducted by its customers from law enforcement and regulatory agencies.

It is FINUS' policy to comply with each lawful request, including but not limited to legal process, and all other lawful inquiries in a timely fashion and to otherwise cooperate fully with law enforcement and other government agencies within the confines of applicable federal, state and local laws and regulations.

If FINUS is served with a subpoena, summons, search warrant or other legal process, or if a government agency otherwise requests information or documents involving money laundering, terrorism or terrorist activity, or other criminal activity, the matter must be referred immediately to FINUS' corporate counsel. Corporate Counsel and the Compliance Officer are authorized to respond to legal process or other requests 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 money laundering and anti-terrorism statutes, licensing issues, and related matters.

Written inquiries, including legal process, seizure notices and forfeitures notices involving money laundering, terrorism, other criminal matters, and licensing issues, received by FINUS' employees must be delivered on the day of receipt to Corporate Counsel or the Compliance Officer. Telephone inquiries must be transferred immediately to the Compliance Officer or Corporate Counsel on the day they are received.

FINUS does not accept verbal requests for information. The Compliance Officer or Corporate Counsel will not respond to any telephone inquiry or oral request for information unless the request is followed by a proper subpoena, other legal process or written request.

National Security Letters

Receipt of a National Security Letter is to be treated with the utmost confidentiality. Only the Compliance Officer or Corporate Counsel are authorized to receive a National Security Letter and must not share the information about such receipt with any party. The Compliance Officer or Corporate Counsel responds to the National Security Letter as directed and maintain records of such National Security Letters in a secured location separate from other legal processes or AML & CTF compliance program records.

Nature and Timing of Response

Corporate Counsel or the Compliance Officer replies in writing to each subpoena or other lawful legal process. The written reply includes: (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, is maintained in the Subpoena/Official Request File. Each reply is 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 is kept in the Subpoena/Official Request File.

Recordkeeping

A written record is made of all telephone and other verbal inquiries from government officials. Each record includes 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 Insight employee receiving the inquiry, a summary of the inquiry, and the action taken with respect to the inquiry. Records of telephone calls and other verbal inquiries from government officials are maintained by the Compliance Officer in a designated file for a period of five years.

A separate individual Subpoena/Official Request File is created for each subpoena, other legal process or written request received that relates to possible violations of money laundering or anti-terrorism statutes, and related criminal activity. Each Subpoena/Official Request File is maintained by Corporate Counsel for a period of ten years from the date the last document is provided to the government in response to the subpoena, other legal process or written request.

Government Subpoenas;

It is the policy of FINUS to comply with all government issued subpoenas. The Compliance Officer along with outside counsel reviews any subpoenas or requests for information to determine:

- Whether the subpoena or request for information was properly served
- If compliance with the subpoena is required
- If the Right to Financial Privacy Act (the RFPA) is implicated

If it is determined that the subpoena or request for information was properly served, the Company takes the following steps:

- An internal file is opened for the maintenance of the subpoena or request
- A review of the subpoena or request is made to determine applicable information to be provided
- Documents requested are gathered and photocopied
- Documents are forwarded to the appropriate authorities
- A copy of the subpoena or request, along with a copy of all documents provided, are kept in the internal file. Additionally, the date all information which was provided is logged in the file along with any names and identification of any regulators or law enforcement representatives who have had communication with the Company related to the subpoena or informational request
- The internal File is kept for a period of 5 years from submission

Information related to any subpoena or request is not divulged to anyone other than the Compliance Officer or Senior Management. Section 1510 of Title 18, US Code, makes it illegal for the Company or any employee, representative, or agent of the Company to directly or indirectly notify a customer or client whose records are being sought by a grand jury subpoena, or notify anyone mentioned in such a subpoena, or to disclose any information that the Company may have provided or disclosed in response to any subpoena or request.

Internal Revenue Service Title 31 Examinations

As an MSB, FINUS routinely undergoes examinations from the IRS under Title 31. Title 31 examinations must be received by FINUS in writing. The Company does not accept any verbal or oral notices of undergoing an examination from the IRS. When a written notice is received, the Compliance Officer will make a copy of this notice. After a copy if made, the Compliance Officer will do the following:

- Notify Senior Management of the Title 31 Examination.
- Gather all documentation for the Examination Period, including all written requests for information or documentation.
- Completes the pre-examination questionnaire provided by the Internal Revenue Service.
- Provides the IRS with any documentation explicitly requested prior to the examination being conducted.
- Corresponds with the IRS regarding the date and time of the examination, and documents all correspondence.

During the examination the Compliance Officer will:

- Acts as the Representative for FINUS to the IRS Agent.
- Document any issues, violations, exceptions, or recommendations raised
- Address any examination issues raised.

Upon Completion of the Examination the Compliance Officer will:

- Notify Senior Management of the Examination results.
- Respond to the examination, either accepting or rejecting their findings.
- Be responsible for implementing any corrective or remedial actions in which FINUS agrees with
- Document any corrective or remedial action taken as a result of the examination.