CREATETRADE® CAPITAL

Anti-Money Laundering (AML) Compliance Program

ADOPTION OF THE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

STATEMENT OF POLICY

1. The Company supports the fight against money-laundering and terrorism by adopting this AML Compliance Program to prevent the Company's business activity from being used to promote such criminal activities.
2. The Company will fully comply with both the intent and letter of all laws and regulations relating to AML, the prevention of terrorist financing, and economic sanctions, including, but not limited to the Bank Secrecy Act (BSA), the USA PATRIOT Act, The Office of Foreign Assets Control (OFAC), and Florida State specific AML Regulations.
3. The Company will train directors, managers and employees to understand and comply with these laws and regulations, and with the content of this AML Compliance Program.
4. The original of this AML Compliance Program will be kept at the main office of the Company located at: 101 NE 3rd Avenue, Suite 1270, Fort Lauderdale, FL 33301, kept in a place accessible to all its directors, managers and employees. Future Company's branches will have copy of this Program, kept in a place accessible to all its directors, managers and employees, as well.

AML COMPLIANCE OFFICER RESPONSIBILITIES

The main AML Compliance Officer's responsibilities include:

1. Ensuring ongoing compliance with Federal and Florida State specific AML regulations.
2. Implementing, reviewing, and updating this AML Compliance Program as necessary due to changes in laws or regulations, and ensuring that all the Company directors, managers and employees have been advised of these changes.
3. Ensuring that the AML Compliance Program is subjected to annual independent reviews.
4. Ensuring all the Company's directors, managers and employees are trained on AML compliance requirements between the next 30 days of initiating their relationship with the Company.
5. Ensuring annual ongoing AML training is conducted in an effective manner for all directors, managers and employees.
6. Ensuring all training is documented, including the date of the training, name of the trainer, the trainee and topics discussed.
7. Implement a "Know Your Customer (KYC)" process to avoid customers that could put the Company at risk.
8. Ensure to establish procedures to monitor and review customer's transaction activities, in order to identity suspicious, high-risk, or otherwise out of the ordinary transactions.
9. Ensure compliance with The Office of Foreign Assets Control (OFAC).
10. Ensuring accurate record keeping and reporting, as mandated by the BSA and Florida State specific regulations.
11. Cooperating with law enforcement reviews, audits and investigations.

INDEPENDENT REVIEW OF COMPANY'S AML COMPLIANCE PROGRAM

The Company must arrange for periodic independent reviews of its AML Compliance Program. This is required by Federal AML Regulations.

1. The Independent Reviews will be conducted by a person or persons who are knowledgeable about the AML requirements.
2. The Company's Independent Review cannot be conducted by the Company's designated AML Compliance Officer, or a person reporting to the AML Compliance Officer.
3. The AML Compliance Officer will ensure that the independent review of the Company's AML Compliance is conducted per schedule, one a year.

DIRECTORS, MANAGERS AND EMPLOYEE TRAINING REQUIREMENTS

1. Training must be provided to all directors, managers or employees, between the next 30 days of initiating their relationship with the Company. At minimum the training must include:

a. Review of all requirements in this AML Compliance Program.
b. Understanding and recognizing money laundering and fraud.
c. Verifying customer identification.
d. All relevant transaction monitoring requirements.
e. Identifying suspicious activity.
f. Reporting requirements related to transactions.
g. Recordkeeping requirements.

2. The AML Compliance Officer, and all directors, managers and employees should also receive an annual ongoing AML training.
3. Additional targeted training should be provided to all directors, managers or employees based on, but not limited to, changes in government regulations, or changes in the AML Compliance Program.
4. A director, manager or employee should also receive additional AML training in the event of a performance issue related to an AML incident.
5. The training must test the trainee to confirm the understanding of the training provided.
6. All training must be documented and retained for at least 5 years.

KNOW YOUR CUSTOMER (KYC) PROCESS

One of the most effective ways to protect the Company from becoming a victim of financial crimes starts with confirming the identity of the customers and really knowing with whom the Company is doing business. To avoid financial transactions that could put the Company at risk, the Company will implement a 'Know Your Customer (KYC)" process that includes, but is not limited to:

1. Completing a Business Profile of the customer when initiating to do business with the Company, containing identifying information that enable the Company to form a reasonable belief that it knows the true identity of each of the Company's customers. The Business Profile may include:

    a. For individual customers: name, address, date of birth, Social Security number and occupation of the individual.

    b. For legal entities customers: business type, incorporation or registration information, certificate of filing, EIN, services offered or products sold, identity of the customer's owner(s) with 25% or more of the equity interest of the customer, and identity of the individual(s) with significant responsibility for managing the customer.

2. Only accepting valid, government issued photo ID documents, such as a driver's license, passport or alien identification card that contains the customer's name, address and photograph.
3. Updating the Business Profile annually.
4. Monitoring the business activity of the customer with the Company regularly.

GOVERNMENT WATCH LISTS. OFAC

The Company will verify customers, beneficial owners and managers against the government watch lists, as prescribed by OFAC. The Company will use the official OFAC webpage https://sanctionssearch.ofac.treas.gov/ to perform this action.

The AML Compliance Officer will conduct a deeper review on possible matches to determine if the name, date of birth, tax identification number, address or other identifiers are truly a positive OFAC match. The records related to each comparison will be retained for at least five (5) years.

REPORTING SUSPICIOUS ACTIVITIES

Suspicious Activity Report (SAR)

All the Company personnel are expected to detect suspicious activity. Upon detecting suspicious activity, the Company personnel should notify the AML Compliance Officer. The AML Compliance Officer will review and investigate the case, which includes determining whether or not to file a SAR before Financial Crime Enforcement Network (FinCEN). The Company's Senior Management determines if the relationship with the customer should remain, or be terminated.

The Company will file the SAR through FinCEN BSA E-Filing System, no later than 30 calendar days from the date an appropriate review of the case is conducted and a determination is made by the AML Compliance Officer that the activity under review is "suspicious" within the meaning of the SAR regulation. To be able to file SARs through FinCEN BSA E-Filing System, the Company will become a BSA E-Filer at http://bsaefiling.fincen.treas.gov/main.html

The AML Compliance Officer will report SAR filing activity to the Board of Directors.

The AML Compliance Officer will retain copies of the SAR and related documents for five (5) years.

If the Company or any of its directors, officers, employees, or agents is subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i).

MAINTENANCE OF RECORDS

Consumer Privacy

In accordance with the Privacy Act the Company will maintain appropriate safeguards for nonpublic personal information that it can collect from its customers.

1. The Company will avoid exposure of identification data such as addresses, telephone numbers, social security number, etc. to any third party.
2. The Company will never share information among its customers.
3. All documents that contain consumers' private and personal information will be stored in a secure location.
4. Any document containing consumer's nonpublic information must be shredded before disposing of the document.

Record Retention

All record keeping and reporting documentation required by the BSA and Florida state specific regulations will be maintained for a minimum of five (5) years and they will be made readily available to the U.S. Treasury Department and/or representatives from other government officials upon legitimate request.

COMPLIANCE TO GOVERNMENT LAW ENFORCEMENT

Government regulators and law enforcement agencies may seek information and records from time to time. The Company will assist these entities in their investigations, provided the request(s) is / are conducted in a lawful manner. Furthermore, government agents are not permitted to use their summons authority to go on unwarranted "fishing" expeditions in the Company records. The Company's employees should not feel pressured by government agents to release customer or Company information without first receiving a proper summons, subpoena or court order.

Upon determination that the request is of routine nature or the procedures for handling the request has been approved with the legal counsel, if needed, the AML Compliance Officer shall proceed with the response. The answer to the request will only contain the information identified in the request and will be provided within the requested time frame.

Whenever possible, the AML Compliance Officer will request a Certificate of Compliance, pursuant to section 4317(c) of the Right to Financial Privacy Act of 1978.