
AML / KYC policy

1. Goals

Money Laundering / Financing terrorism (AML / KYC / CFT) refer to processes that involve covert financial transactions made to give illegitimate money, accrued through illicit means such as embezzlement, corruption, illegal gambling, terrorism, organized crime, the appearance of having been legally earned. In the broadest terms, the method by which money is laundering involves three phases:

- (a) Placement – the accumulation of hard, physical cash earned through illicit means.
- (b) Layering – distributing the funds to be laundered across a convoluted, multi-layered network of financial transactions specially arranged to cover the launderers' tracks by obfuscating the audit trail.
- (c) Integration – lending an air of legitimacy to funds accrued through illegitimate means.

Assuming the layering stage was a success, integration involves funneling the illicit funds back into the legitimate economy so as to give them the appearance of clean, legitimate earnings.

The primary goal is to obscure the actual origins of the illegitimate funds, making it possible to dispose of them without legal repercussions. This involves lending them the appearance of legally accrued funds by passing them through several ostensibly legitimizing financial transactions. Money launderers have benefited greatly from new technologies which they have enthusiastically made use of to move money globally at greater speeds, creating serious challenges for those endeavoring to track and prevent their activities. Authorities around the world have highlighted attempts to abuse the financial system in order to commit fraud as a serious issue requiring constant, ever-adaptive vigilance.

We are an upstanding company that sees it as our ethical duty to society and the economy to forestall the abuse of the financial system in terms of money laundering. We support coordinated worldwide efforts to combat money laundering. In this struggle, it falls to us to uphold strict Know Your Customer policies.

Doing our part to contribute to the global financial community's determined efforts to combat money laundering, we have committed to running our daily business activities with the highest standards in professionalism, attention to detail, and due diligence. We are constantly striving to adhere to both the letter and the spirit of applicable legislation, policies, regulations, and guidelines for best practices.

The goal of our efforts in Anti-Money Laundering/Combating financing terrorism is to prevent our resources from being exploited in any way for the said illicit purposes. As such, among our AML / KYC / CFT policies are:

- Customer Identification Measures – Know Your Customer policies.
- Surveillance of suspicious transactions.
- Delegation of duties to monitor compliance.
- Staff Training.
- Rigorous maintenance of Records.
- Regular verification of full adherence to our AML / KYC / CFT and Compliance policies.

Our “Customer due diligence” (CDD) measures involve:

- (a) Identifying each customer;
- (b) Ascertaining whether a given customer is representing a third party and, if he/she is, identifying the third party;
- (c) Verifying the identity of the customer and any third party on behalf of whom the customer is acting;

These policies and measures are to be adopted by all of our branches, offices, counteragents, and affiliates and are to be implemented in concert with the associated operational guidelines that are occasionally put into practice.

Such policies outline the obligations of both managers and employees to:

- Formulate and implement policies, measures, and monitoring on the approval of customers and support for and surveillance of them.o

- Customer due diligence.o

- Refusing or ceasing business relationships or transactions.o

- Staff training on approval of, support for, and surveillance of customers.o

- Surveillance of accounts, actions, policies, procedures, and plans.o

- Awareness and communication.o

- Managerial reporting.o

- Submitting Reports (SAR/STR) to the Financial Intelligence Unit (FIU).o

Key Principles and Objectives

The primary goals and of this manual are as following:

- To ensure we implement all policies and measures required to guarantee the maximal prevention of money laundering, proliferation financing, and the financing of terrorism and similar in our customers’ use of our services.o

- To formulate and implement all legally required customer due diligence measures and ensuring they extend to all business relationships and transactions.o

- To ensure that before a working relationship is established with a potential customer, the latter has submitted all necessary data to us. All data submitted must be confirmed against data gleaned from other sources as per the applicable laws.o

- We may refuse to establish, or cut off, any business relationships or transactions in which there are any apparent risks that our services or infrastructure will be misused for money laundering and/or terrorist financing.o

- The Company will ensure that all affected staff members receive the necessary training on approving, offering service to, and surveilling customers.o

- The Company shall vigilantly surveil compliance with this manual, and all responsibilities it implies as required by law.o

- All relevant staff members shall be briefed on the stipulations of this manual, particularly their obligations and the measures that they are to take.o

- For the company to vigilantly and successfully surveil measures regarding the approval, provision of service, and surveillance of customers, detailed managerial reports must be prepared.o

2. Compliance duties

At the Company, compliance duties fall into two levels, that is, the obligations of the Money Laundering Reporting Officer and those of the Money Laundering Compliance Officer.

The CEO (who also takes on duties as a Money Laundering Reporting Officer) and the Company's Board of Directors.

The duties of the CEO and the Board of Directors include:

- I. Nurturing a corporate culture conducive to reaching success in compliance goals by guaranteeing vigilance in the hiring, selection, personal development, and surveillance of compliance staff.
- II. Facilitating and nurturing a thorough awareness of the urgency of the issue of compliance with AML / CFT / KYC policies, among the Company's staff at every level.
- III. Monitoring the creation, constant development, and practical application of policies and measures in the field of compliance.
- IV. Ongoing, intensive collaboration with the Compliance department to guarantee that that relations between the Compliance Department and the members of the Board are smooth and conducive to success in this field.

2. The Company's Compliance department, led by the Chief Operational Officer (who also takes on the role of Money Laundering Compliance Officer).

The duties of the Money Laundering Compliance Officer include:

- I. Appointing compliance officers (the staff of the Compliance department);
- II. Surveilling, organizing, and monitoring the daily work of the compliance officers.
- III. Providing training for the compliance officers.
- IV. Reporting to the CEO and the Company's Board of directors if the Compliance department has discovered signs of a fraudulent transaction that may be related to money laundering.
- V. Regular monitoring of the practical application of AML / KYC / CFT policies and compliance measures.
- VI. Keeping this manual up to date based on the results of regular appraisal of its relevance.

The duties of the Compliance department are:

- I. To enact the monitoring required to detect fraudulent transactions.
- II. Revoking or preventing any such transaction.
- III. Receiving disclosures from personnel or other sources on any transactions showing signs of fraud.
- IV. Training personnel and drafting detailed instructions on identifying potentially fraudulent transactions.

3. Know your customer measures

The security of our customers is a top priority. As such, we regard our duty to protect our customers'

interests as our highest duty.

The Company has put a set of KYC (Know Your Client) measures into practice. These have been developed to ensure the security of our customers' sensitive private data and to ensure that the company's procedures adhere to the best practices in the financial services industry. Such measures are intended to preempt any attempts at identity theft, money laundering, fraud, or terrorism.

The company has adopted a stringent Zero Tolerance policy. Each instance of potential fraud is to be recorded and instantaneously halted, while any trading accounts involved will be blocked and, if fraud is confirmed, closed. The balance of all such accounts will be requisitioned.

Such measures ensure the security of our customers' personal data and financial transactions. If a customer has not fully undergone our KYC measures, his/her trading activity will be restricted, and he/she will be unable to withdraw money from his/her account.

To open and credit a trading account with the company, a potential customer must provide the following documentation:

Government-issued Proof of Identity (colored photo or scan), such as:

Passport
National Identity card

Such ID must be clear and legible and include the information below:

Full name
Date of birth
Date of issue and of expiry
A Clear photo

The ID document must be valid for six months from the time of submission.

2. Secondary proof of identity, (color photo/scan), such as:

Driver's license
Insurance document
Certificate of birth/marriage/divorce
Educational degree
Military ID

3. A color photo/scan of a document that verifies your residential address. The document must have been issued within 90 days of the time of submission. The photo/scan must display your residential address in full, your full name, its date of issue, and official stamp or identifying QR/barcode. Such documents may include a:

Utility bill
bank statement

check
residence permit
penalty notice
legal contract

4. The customer must submit color photos/scans of both sides of the signed debit card(s) he/she intends to use to make deposits. For the customer's security, he/she is advised to conceal the CVV number and the seventh to twelfth digits of the card number(s). This should leave the first six digits and the final four digits on either side of the card(s) visible. All other information on the card must be visible, particularly the card holder's name and the expiry date.

The documents listed above are to be provided in the PDF, JPEG, JPG, or PNG format by sending them to the Compliance Department at: dispute@growline.email.

Send in your KYC materials at your earliest convenience upon opening your trading account. Please note that your missing compliance may result in limitations on your trading account.

Note that in the absence of the KYC materials outlined above, the company will be unable to process any requests to make withdrawals from your trading account.

Surveillance of withdrawal requests

The Company's policy on withdrawals is:

- The Customer has the right to withdraw money at any time. Any bonuses awarded to the customer from the company can be withdrawn in accordance with certain requirements outlined in the corresponding promotional campaign.
- The Customer must submit a signed withdrawal application form to the Company.
- The sum requested has to be withdrawn to the account that served as the source of the money corresponding to the withdrawal request. For instance: if the Customer deposited the funds by wire transfer, then the withdrawal must also be made by wire transfer to the originating account. Likewise, if the funds originated from a credit card, they are to be withdrawn to the corresponding credit card. The same logic applies in other instances.

The compliance procedure for each type of withdrawal is delineated below.

Compliance procedures in place per method of withdrawal used by a Customer

Step	Transaction/function	Responsible officer	Result
1.	Customer submits a signed withdrawal form to the Company	The officer responsible for Customer Retention.	Verify the withdrawal form and move on to Step 2.

<p>Verify the Customer's identity (ID, telephone number, and other details). Verify that the Customer's account has sufficient balance for the withdrawal and, if a bonus is to be withdrawn, that the Customer is in compliance with the stipulations of the corresponding promotional campaign.</p>	<p>The officer responsible for Customer Retention</p>	<p>If verification of identity and confirmation are successful, forward the withdrawal form to the Compliance Department. If not, notify the customer.</p>
<p>3. Verification of the Customer's identity, review of the transactions recently made by the Customer, identification of the correct withdrawal method.</p>	<p>The Compliance Department. CEO (if necessary) The Board of directors (if necessary).</p>	<p>If it passes review – forward the withdrawal form to the Financial Department to carry out the withdrawal. In the event of any problem, the Compliance department can return the form to the officer responsible for retention to request extra info from the Customer. In high-risks scenarios, the Compliance Department can notify the Company's CEO. In such an event, the CEO is given the ultimate decision regarding the withdrawal unless the particularities of the situation call for it to be referred to the Board of directors.</p>

All transactions showing signs of potential fraud should be reported to the Compliance Department before being carried out, wherever possible. A detailed report on all such transactions, whether carried out or not, are to be reported to the Compliance Department.

Any transaction showing signs of potential fraud discovered before being completed may only be completed with the Compliance Department's approval.
Within reason, the Compliance Department is to have access to all data/documentation that may be required to fulfill its duties in a full and vigilant manner.

It is the duty of the Compliance Department to notify the CEO of any activity showing signs of potential fraud. The CEO, in turn, is responsible for escalating any particularly concerning activity to the Company's Board of Directors.

The Board of Directors has the authority to decide:

– escalate any particularly concerning activity to the Financial Intelligence Unit (FIU) through a Suspicious Activity Report (SAR) or a Suspicious Transaction Report (STR). Such reports, SARs and STRs, feature thorough data on transactions showing signs of potential fraud. The forwarding of SARs and STRs are meant to aid the relevant governmental agencies to determine which people, groups, or organizations are engaging in fraud, terrorist financing, money laundering, or other illicit activities. An SAR, in particular, is intended to report suspected or established illegal activity the company has uncovered through its surveillance measures;

– take proportionate action required to identify the goal of the transaction, the source and final destination of the money transferred, and to identify and locate, the ultimate beneficiary.

4. Staff training

The Company offers onboarding and constant training for employees engaged in KYC measures to ensure they operate with utmost competence. Such training varies in duration and content as per the needs of the staff being trained and the roles they are to fill. The structure and goals of such training are tailored for the target audience, whether new hires, customer-facing personnel, or those working in customer retention.

New hires are trained in the fundamentals of our AML / CFT / KYC measures and why such measures, and adherence with all related policies, are vital for the Company. They are trained in the fundamental requirements of compliance in a two-week onboarding program attended by every new hire. Customer-facing personnel undergo training in confirming the identity of new customers, following due diligence procedures in dealing with the accounts of established customers, and vigilantly endeavoring to identify any suspicious behavior.

At certain intervals, training is offered to update and refresh staff member's competency and to ensure they are up to speed on recent developments in the field.

It is vital that all personnel involved in the field take the imperative to constantly maintain KYC measures with the utmost seriousness. The success of such measures is predicated upon a corporate culture formed around such an understanding and earnest approach.

Repercussions for Non-Compliance

The Company's personnel must adhere to the compliance procedures and measures as described in this manual.

Any oversight in such compliance can lead to dire repercussions, taking the form of disciplinary action or even criminal prosecution of a particular staff member.

Communication with Employees

The Company has established open, readily available channels of communication between the Compliance Department and all of the Company's staff members. Regular internal news on AML / CFT / KYC is offered to all personnel. The Company provides onboarding and ongoing training for its employees to ensure full adherence to the compliance procedures.

The goals of such training are tailored for the target audience, whether customer-facing personnel, compliance personnel, or retention personnel. This ensures that everyone involved fully understands the reasoning for the compliance measures and procedures and upholds them with vigilance.