XFLOW
MARKETS

Client due diligence and onboarding Policy

CLIENT DUE DILIGENCE AND ONBOARDING POLICY

XFLOW MARKETS LLC

1. Introduction

This policy sets out the Customer identification and verification procedures (also referred to as "Know you Customer" or "KYC" procedures) of XFLOW MARKETS LLC. (hereinafter referred to as "XFLOW"), incorporated in Saint Vincent and the Grenadines (hereinafter referred to as "SVG") with number 255 LLC 2020.

The Internationals Anti-Money Laundering and Anti-Terrorism Financing (hereinafter referred to as "AML/CFT") regulations requires any Reporting Entity (such as XFLOW) to carry out procedures to verify a customer's identity and other required information **before** providing any service to that customer.

Furthermore, ongoing due diligence of customers must be conducted. Where a review of a customer, business line or other circumstance results in a **change in the risk profile** of an **existing** customer, then the customer identification procedures described in this policy are required to be implemented according to the assessed risk.

Accordingly, the primary purpose of this policy is to set out the applicable customer identification and verification procedures for customers of XFLOW.

2. KYC Responsibilities

The client relationship managers (or other Representatives responsible for the client) have full responsibility for knowing their customers. Thus, the KYC process, including the initial and ongoing due diligence measures, shall be carried out by the businessperson responsible for each client.

XFLOW's compliance unit has the responsibility to develop the KYC rules and ensure that they are up to date. Furthermore, Chief Compliance Officer as well as AML/CFT Compliance Officers shall advise and supply the client relationship managers with information and regular training in relation to KYC matters, perform monitoring of KYC procedures including sample selected client reviews and engage in other AML/CFT risk management activities as defined herein.

The main components of the KYC process are:

1. Gathering Basic KYC information (including identity check),

2. Checking against sanction and other lists,

3. Assigning risk and due diligence level,

4. Applying enhanced due diligence measures,

5. Customer adoption process, and

6. Ongoing customer due diligence.

3. Gathering KYC information (including identity check)

The level of information which must be collected is risk based, i.e. dependent on the identified ML/TF risk posed to XFLOW having regards to the following factors:

(1) Its customer types, including any Politically Exposed Persons

(2) The types of designated services provided;

(3) The methods by which the designated services are delivered;

(4) The foreign jurisdictions with which it deals.

There are different customer identification and verification procedures for different customer types. Customer types include:

1. individuals (natural persons);

2. legal persons (companies, incorporated associations, registered co-operatives, government bodies);

3. legal establishments (trusts, partnerships, unincorporated associations).

The client relationship manager shall, for each customer who seeks to become a client of XFLOW, gather a certain minimum level of KYC information, referred to as Basic KYC information and for the high-risk customers perform enhanced due diligence which includes collecting additional information. Gathering of information also includes verification of the customer's identity. In addition, the general principles defined in this Program shall be applied.

If there are gaps in the Basic KYC information or if ambiguity or uncertainty occurs in relation to the information provided by a customer, additional questions shall be asked, or additional documentation requested. Where the identity of the customer cannot be confirmed without doubt, or information on beneficial ownership and purpose and intended nature of the business relationship cannot be obtained, a business relationship **shall not be entered into**. In such cases, transactions initiated by the customer shall not be carried out.

Where the customer is introduced by a person acting as the customer's agent, customer identification procedures are to be undertaken in respect of both the agent and the underlying customer i.e. XFLOW considers both the investor and the agent as its customer.

XFLOW shall not keep anonymous accounts. The identity check concerning a private individual or anyone representing a legal entity shall as a minimum include a review of identification documents such as a generally approved identity card or passport.

In the case of both private individuals and legal entities, risk-based measures shall be taken to establish the source of funds and beneficial ownership of assets involved. Beneficial ownership shall be established for all customers.

In the case of legal entities, trusts and similar arrangements, reasonable measures shall be taken to understand the ownership and control structure of the customer.

Reliable and independent documentation (original documents, certified copies) as well as other available reliable sources (public electronic data, data warehouses etc.) shall be used to verify customer identity and other information provided. For client identity verification only original documents or duly certified copies shall be appropriate, copies are acceptable only for additional supporting documents.

3.1. Non-face-to-face customers

XFLOW shall apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

In order to mitigate the higher risk which may arise due to non-face-to-face customer XFLOW shall apply additional risk reducing measures such as: require certification of documents presented or additional documents to complement those which are required for face-to-face customers, initiate independent contact with the customer, use third party introduction, seek verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds etc.

3.2. Correspondent banking

XFLOW shall gather sufficient information about their respondent banks to understand fully the nature of the respondent's business before starting the correspondent banking relationship.

The information required shall include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third-party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country.

XFLOW shall only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

XFLOW shall not enter into or continue a correspondent banking relationship with a Shell Bank. Furthermore, appropriate measures shall be taken to ensure that XFLOW does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a Shell Bank.

4. Checking against sanction lists etc.

Specific regulatory restrictions and sanctions regarding certain subjects and/or jurisdictions must be observed (e.g. EC regulations passed from time to time with respect to particular political or terrorist entities, OFAC sanctions etc.). In addition, based on a risk assessment and relevant legal prerequisites, new and existing customers shall be checked against relevant external and/or internal watch lists.

XFLOW strictly follows the sanctions imposed in the jurisdictions in which it operates and sanctions of international institutions and regulatory bodies. If there's a sanction applicable to the customer or party of the transaction, it will restrict XFLOW from doing business with those certain individuals, entities and countries.

All monetary transactions and related data (accounts, involved parties) are to be individually and manually screened against sanctions lists. XFLOW will use third party service providers for sanction screening solution, which is updated regularly and covers several sanctions, watch, regulatory and law enforcement lists (including, but not limited to: OFAC, EU, UN, UK HMT).

The sanction screening strictly applies to every incoming and outgoing payment and is performed manually by the Representative in XFLOW responsible for the transaction (client relationship manager and in certain cases AML/CFT compliance officer).

Where a positive result is returned in respect of a customer i.e. the name appears on the relevant list, the AML/CFT Compliance Officer must be notified immediately and is responsible for overseeing the ongoing treatment of the customer and where applicable, making all reports, liaising with enforcement offices and reporting to the Board.

Any requests for third party payments will require that the name of the third party to be identified, verified and checked. Where a positive result is returned in respect of a third party payee i.e. the name appears on the relevant list, the AML/CFT Compliance Officer must be notified immediately and is responsible for overseeing the ongoing treatment of the customer and where applicable, making all reports, liaising with enforcement offices and reporting to the Board.

XFLOW relies on the information provided by the customer or information from other financial institutions unless it gives rise to suspicion that the information is unreliable or dishonest. Removing or falsifying any information that would identify that a customer or a transaction may be covered by a sanction is strictly prohibited.

Although based on the specifics of XFLOW's client base and volume of the transactions performed manual checks of every single transaction is an acceptable routine, additionally automated transactions screenings will be available with the launch of new core IT system of XFLOW. The software will inter alia, include tailor-made AML software with the functionality of an AML alert system, integrated with renewable external World Check's database (for sanctions lists and other available information) and enhanced by internally developed criteria and scenarios (such as certain threshold amounts, search words and other automatic features) triggering automatic AML alerts to responsible people, automatic FIU report filing, payment freeze feature etc. The system will also allow for the creation of White Lists and will have other features created to augment the due diligence level and automate some of the manual operations of XFLOW. After the launch of the AML alert system, the process and procedures on the features will be described separately or this policy shall be updated.

All customers and beneficial owners must be screened against applicable sanctions during the client take-on and continually over the course of the relationship. Depending on the individual, entity or country involved, transactions/accounts/assets of sanctioned parties must be blocked.

In addition, if a legal entity customer is assigned enhanced due diligence, the directors, authorized signers and powers of attorney related to the customer have to be screened, initially, in conjunction with client take-on, and risk-based on an ongoing basis.

Any breach of sanctions regimes must be reported to the competent authorities in accordance with local laws or regulations. In such cases Chief Compliance Officer shall be notified. XFLOW shall keep a logbook of accounts whose funds have been frozen.

5. Assigning risk and due diligence level

Representatives must assess that a customer's risk profile as being high, medium or low.

If the customer's profile is ranked as high risk, further enhanced due diligence procedures must be applied as described herein.

The following circumstances shall indicate the high risk and enhanced due diligence level accordingly:

5.1. A check against a sanction list or watch list reveals that the customer or persons associated with it potentially may be listed on one or more lists,

5.2. Circumstances indicate that the customer (or persons associated with it, in the case of a customer that is a legal entity) is a PEP,

5.3. The customers´ behavior or other circumstances indicate high risk,

5.4. The customer, following the risk ranking procedure, is seen as representing high risk, e.g. due to customer-, country-, product and services- and/or combination risks;

5.5. Other risk variables as indicated in paragraph below trigger high risk.

6. Applying enhanced due diligence measures

Based on an assessment of ML/TF risk XFLOW has identified certain risk variables which **will** trigger the requirement for additional KYC information and verification procedures to be performed (these depend upon customer type and that customer's risk profile).

The risk variables are:

(1) Where the prospective customer (natural person, director, member of governing body, beneficiary or beneficial owner) is named in a government list or a credible source's list;

(2) Where the risk of terrorism is identified;

(3) Where the customer, who is an individual (natural person), is a PEP or is known to have a link to a PEP;

(4) Where a non-natural person is a PEP or is known to have a link to a PEP (this includes any directors, beneficial owners, beneficiaries and agents as the case may be);

(5) Foreign jurisdiction risk (individuals and non-natural persons) i.e. the place the customer is domiciled (located) is considered high risk. In the case of non-natural person this includes officers and beneficial owners and beneficiaries;

(6) In the case of a listed company, the foreign jurisdiction risk with respect to the location of the exchange on which the listed company is traded;

(7) The customer has sophisticated activities and/or has links with high risk foreign jurisdictions;

(8) The customer's business activities place it in a higher risk category;

(9) Where intermediaries exist that are not Reporting Entities;

(10) Where the prospective customer is not physically present for identification purposes;

(11) Complex customer structures with numerous layers e.g. trusts;

(12) The customer structure does not support the disclosed business of that customer e.g. in the case of partnerships; (13) Products & services risk;

(14) Services are provided exclusively via the internet.

The Enhanced Customer Due Diligence must always be applied when:

1. The Bank determines under its risk-based systems and controls that the ML and TF risk is high; or
2. a suspicion has arisen for the purposes of the AML/CFT regulations (suspicious transaction, suspicious activity, transaction conducted by money laundering entities, transactions involving terrorist property, transaction with no legitimate purpose); or
3. a party to the transaction, which the Bank is entering into or proposing to enter into, is physically present in, or is a business incorporated in, a prescribed foreign country (country linked with terrorist organizations).

With regards to high risk customers and/or business transactions the following measures shall be applied by the Representatives:

1) regularly collect information from the customer or from third party sources in order to update Banks knowledge (derived from the enhanced identification process) of the customer (i.e. conduct regular reviews of the customer information);
2) undertake more detailed analysis of the customer information including examining as far as possible the background and purpose of the transaction and business relationship;

3) regularly verify or re-verify the customer information in accordance with the
   a. customer identification process;
4) undertake more detailed analysis and monitoring of the customer's transactions - both past and future, including, but not limited to:
   a. the purpose or nature of specific transactions; or
   b. the expected nature and level of transaction behavior; 5) seek
   senior management approval for:
   a. establishing or continuing with a business relationship with a customer; or
   b. whether a transaction on an account should be processed; or
   c. whether the service should commence to be provided or continue to be provided to the customer;

Furthermore, for a customer ranked as high-risk customer the measures deemed relevant of the following shall be applied (the measures listed under 1 and 2 below are obligatory every time):

1. Verification of the beneficial owners by reviewing supporting documents on beneficial ownership information provided by the client or third parties, such as shareholders ledger, and verification of the identity of the beneficial owners by requesting a copy of the beneficial owner's identity card or passport,

2. Screening the customer, beneficial owners and representatives of the customer against World Check's lists (sanction, PEP-lists and other watch lists),

3. Ask additional questions and request additional documentation, based on identified risks, ambiguities and uncertainties,

4. Take adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship,

5. Supplementary measures to verify the documents supplied, or require confirmatory certification by a credit- or financial institution,

6. Other appropriate measures (communication with several representatives of the client company etc.).

All enhanced measures applied shall be documented and the records kept.

If after enhanced customer due diligence has been conducted the Representative and/or the AML/CFT Compliance Officer determines that there remains a high risk of ML/TF, or that one of the grounds for reporting a suspicious matter to FIU has been met, the AML/CFT Compliance Officer, in consultation with senior management, will determine whether the circumstances are suspicious enough to warrant the account being placed in suspense or closed and whether it is a further suspicious matter and thus, reportable.

PEP

Specifically, if the potential customer is a PEP it falls into the high-risk category and is subject to enhanced due diligence, enhanced verification and enhanced on-going due diligence procedures.

XFLOW shall investigate thoroughly the source of funds before accepting PEP as the client. Further measures shall be also taken in order to satisfy itself as to bona fides of the intended transactions of a PEP customer.

The handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk. Possible risk factors to consider are:

1. the level of (informal) influence that the individual could still exercise;
2. the seniority of the position that the individual held as a PEP;
3. whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Provided that the above-mentioned risk factors do not trigger any concerns for higher risks, the person shall not be considered a PEP, if he/she has lost his service with prominent public functions more than a year ago.

7. Customer adoption process

After having gathered and verified customer information and assigned risk and due diligence level, irrespective of the level of risk assigned the client relationship manager shall present his proposal to approve the client to the *ad hoc* **Customer Adoption Committee.** The Customer Adoption Committee consists of respective client relationship manager, Managing Director of XFLOW and Chief Compliance Officer, or other AML/CFT Compliance Officer dedicated by him. The customer shall only be accepted if all members of the committee support the acceptance.

In case of disagreement between Customer Adoption Committee members, the client can be adopted only if approved by the Board of Directors.

As regards the customer adoption process the following records shall be kept:

1. When and by whom was a decision taken on establishment of the customer relationship, and
2. If the customer was assigned high risk rank, the reason why, including the reasoning on which the Customer Adoption Committee approved it.

After relevant KYC procedures have been conducted by the responsible client relationship manager the decision to establish correspondent banking relationships with the financial institution falls within the competence of the Customer Adoption Committee.

8. Ongoing customer due diligence

The client relationship manager shall conduct ongoing due diligence of all business relationships to ensure that the KYC information is up to date. It shall be documented when a review was carried out and by whom.

The reviews of existing records shall also be performed when a transaction of significance takes place, when customer documentation standards change substantially, when there is a material change in the way that the account is operated or when client relationship manager becomes aware at any time that it lacks sufficient information about an existing customer.

Periodic reviews shall be conducted:

3. For low risk customers - at 36-month intervals,
4. For medium risk customers - at 24-month intervals,
5. For high risk customers - at 12-month intervals.

The issue of changing the assigned risk level for a certain customer to higher risk or vice versa shall be handled by the relevant Customer Adoption Committee.

Other procedures of ongoing customer due diligence include the following:

1. Customers' transactions will be monitored on an ongoing basis in order to identify any unusual or suspicious activity or transaction;
2. Representatives will review transactions, including trading and electronic fund transfers, in the context of other account activity to determine if a transaction is suspicious;
3. the AML/CFT Compliance Officer (s) will be responsible for monitoring adherence to this Program and the AML/CFT Act, and will report suspicious activities to the appropriate authorities; the AML/CFT Compliance Officer will ensure that a sufficient sample of activity will be selected to enable the identification of matters of concern;
4. exception reports will be utilized to identify possible ML/TF risks and include monitoring transaction size, location, type, number and nature of the activity;
5. employee guidelines, with examples of suspicious money laundering activity and lists of high-risk customers whose accounts may warrant further scrutiny, will be prepared; and
6. The AML/CFT Compliance Officer will conduct an appropriate investigation before reporting a suspicious matter.

In addition to regular reviews, circumstances may arise in which an otherwise low risk customer will be elevated to high risk.

For example, a customer on commencement of the relationship may be classified as low risk. However, after considering the customer's circumstances (such as financial resources) and as a result of a change in activities, the risk profile of the customer may be elevated to high.

In circumstances where the customer's risk profile is elevated, further measures and controls will be implemented to mitigate and manage against potential ML/TF risks, including the following:

1. Immediate notification to all appropriate representatives / business units;

2. Further KYC information and verification procedures performed;

3. An increase in the level on monitoring (i.e. in accordance with the new classification or rating of the customer risk, being medium or high and monitoring intervals commensurate with the identified risk).

9. Employee Due Diligence procedures / checks

There is a requirement within the AML/CFT Act to perform due diligence on certain representatives of XFLOW i.e. staff, employees, contractors, those seconded to the company for an interim period etc. The level of due diligence required depends upon the function performed and level of seniority / work performed.

The employee due diligence program includes appropriate risk-based systems and controls for XFLOW to determine whether to, and in what manner to, screen any prospective employee and also re-screen an employee (where that employee is transferred or promoted) that may be in a position to facilitate the commission of a money laundering or financing of terrorism offence in connection with the provision of a designated service by XFLOW.

The employee due diligence program also establishes and maintains a system for XFLOW to manage any employee who fails, without reasonable excuse, to comply with any system, control or procedure established in accordance with the present policy.

XFLOW has prepared a Recruitment Policy which covers the vetting of candidates for employment, taking and checking of references and the procedures to be followed in the recruitment process (see below paragraph).

The Recruitment Policy requires the Managing Director to conduct a formal interview of the candidate. XFLOW may also perform skills assessment, reference checks or any combination of these prior to offering a candidate a position. Representatives will be selected based on their experience, skills, qualifications and industry knowledge.

The status of all new members of staff must be identified on their commencement of employment (authority to represent the company and provide a designated service) and the identification must be verified and recorded i.e. XFLOW will ensure that the identity and past history of a prospective employee (representative) has been verified prior to employment or authority granted to represent the company.

Once employed (or appointed to represent the company), Representatives that are identified as "high risk" will be subject to closer and more frequent monitoring. This includes monitoring of the representative's customer accounts and relationships (i.e. monitoring will be undertaken more frequently than that prescribed by the regular intervals pursuant to internal review procedures). In addition, these representatives may be subject to transactional limits until such time that comprehensive training in policies and procedures has been completed.

Examples of representatives to be considered as "high risk" include the following:

1. Representatives who are in a position of dealing with customers or circumstances which are identified as high risk.
2. Representatives in "key" positions.
3. Representatives that provide unusual or extraordinary activities.
4. Representatives who fail to conform to the company's compliance systems and/or controls.
5. Staff promoted to more senior levels with greater AML/CFT responsibilities that are yet to complete further AML/CFT training in policies and procedures.
6. Representatives which qualify as "high risk" for other reasons such as for example leading of lavish lifestyles, which cannot be supported by the representative's salary or other practical reason.

The level of staff turnover will also be considered and monitored on a regular basis. Employee accounts are subject to the same AML/CFT procedures as customer accounts, under the supervision of the AML/CFT Compliance Officer.

The performance of supervisors with respect to compliance with the AML/CFT Act obligations will be monitored as part of their annual performance review.

Representatives who fail to comply with the compliance systems and/or controls will be subject to disciplinary procedures, which may include termination of employment (cancellation to represent the company). Representatives that are suspected of facilitating money laundering or terrorism financing will be additionally reported to the appropriate authorities.

10. Intermediary and introduced business

In some instances, XFLOW may rely on the procedures undertaken by other banks or introducers when business is being referred.

Prior to establishing relationship with such intermediary or introducer (hereinafter –intermediary), XFLOW should satisfy itself that the intermediary:

1. is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record- keeping requirements;
2. is fit and proper and is exercising the necessary due diligence in accordance with the standards applicable to XFLOW;

3. comply with the minimum customer due diligence practices as applied by XFLOW;
4. has reliable systems in place to verify the identity of the customer;
5. allows XFLOW to verify the due diligence undertaken by the introducer at any stage.

All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to XFLOW, who must carefully review the documentation provided.

In addition, XFLOW shall conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

XFLOW shall not rely on introducers that are subject to weaker standards than those governing XFLOW's own KYC procedures or that are unwilling to share copies of due diligence documentation.

There must be a written agreement in place for the management of the customer identification records whereby *inter alia* XFLOW has the right to access the records made by the agent and has the right to request information on their compliance procedures applied as well as request copies of the records made by the agent.

11. Client accounts opened by professional intermediaries

When XFLOW has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

XFLOW may hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. XFLOW may also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the international bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

Where the funds are co-mingled, XFLOW should look through to the beneficial owners. There can be circumstances where XFLOW may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as XFLOW. XFLOW shall accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, XFLOW shall apply the criteria set out for intermediaries and introduced business, in order to determine whether a professional intermediary can be relied upon.

Where the intermediary is not empowered to furnish the required information on beneficiaries to XFLOW, for example, lawyers bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this guideline or to the requirements of the AML/CFT Act or anti-money laundering legislation in other jurisdictions, then XFLOW should not permit the intermediary to open an account.

12. Discrepancies

If a discrepancy exists between information collected and verifying documents, then the Representative will take steps to resolve the discrepancy (where possible) and will record the steps taken. Additional measures may include:

1. An explanation from the customer in respect of the discrepancy together with supporting documentation;

2. Copies of transaction records (e.g. recent bank statement within previous two months);

3. Copies of other transaction documents;

4. Copies of management body's decisions;

5. Extracts from public governmental registers or other relevant registration body's certification etc.

The action to be taken will depend upon the discrepancy and will vary according to customer type and that customer's risk profile.

13. Disclosure Certificates

Where information is to be verified and it is not otherwise reasonably available from independent verification sources, a Disclosure Certificate may be provided from the customer (other than where the customer is an individual). This will constitute a reliable and independent document. Under no circumstances can a Disclosure Certificate be relied upon in verifying the identity of a customer where that customer is an individual. The Disclosure Certificates are accepted by XFLOW only for those customers that have been classified or ranked as low to medium risk.

A Disclosure Certificate will not be accepted as suitable evidence to verify information where factors exist which result in the elevation of the ML/TF risk and the customer receives a high-risk classification (ranking).

In cases where a company/trust/partnership/co-operative/association is established in SVG or in other comparable jurisdiction and is subject to regulatory oversight similar to that of SVG in its country of origin and/or principal operations (both have to be comparable jurisdictions), a Disclosure Certificate may be acceptable where information relating to beneficial ownership or other information is not otherwise reasonably available from other verification sources. The copy of the identity document of the beneficial owner shall be always collected as a minimum in addition to Disclosure Certificate. Where the company is not subject to regulatory oversight similar to that of SVG in its country of origin and/or principal operations (non-comparable jurisdiction), a Disclosure Certificate may not be relied upon.

The information provided in Account Opening Form and other related forms filled in and signed by authorised customer representatives are deemed to act as proper Disclosure Certificates. Disclosure Certificate may have any other form acceptable to the Bank.

In these circumstances where the identity cannot be readily verifiable to the reasonably satisfaction of the representative (or agent or intermediary), the matter will be referred to a senior manager, who in consultation with the AML/CFT Compliance Officer, will determine whether XFLOW will enter into a customer relationship.

14. Customer refusing to provide information

If a prospective customer either refuses to provide information when requested, or appears to have intentionally provided misleading information, XFLOW will not accept the prospective customer (i.e. open the account) and will not do business with that person until the information has been provided and the customer identification and verification procedures as contained in this policy have been satisfactorily completed.

If an existing customer either refuses to provide information when requested or appears to have intentionally provided misleading information, then XFLOW, after considering the circumstances and ML/TF risks involved, will consider closing the account.

In either case, the AML/CFT Compliance Officer will be notified in order to determine whether the circumstances constitute a reportable matter and whether the risk classification of the customer should be increased.

15. Forgery

Representatives responsible for the collection and verification of KYC information are not required to necessarily investigate whether a document provided by a customer has been validly issued. For example, representatives (or agents or intermediaries) can rely on documents issued by a governmental or statutory body as reliable and independent documentation and thus, verification of a customer's identity.

If, however, the document exhibits signs of fraud (tampering with the document), then the matter must be immediately reported to the AML/CFT Compliance Officer and he will consider the factors in determining whether XFLOW can form a reasonable belief as to the customer's true identity and whether there's a matter of reporting to official authorities.

16. Recording the collection and verification procedure

Representatives responsible for the collection and verification of customer identification will record the verification procedure, including all identifying information provided by a customer, details of the verification methods used and the results of the verification.

Furthermore, where a discrepancy arises (in the verification process) Representatives shall record the method and result of the resolution of any discrepancy in identifying and verifying information.

Any additional information or verification procedures are to be documented and copies of any supporting documents (evidence) provided by the customer or obtained electronically by Representatives are to be retained as part of the records.

The Account Opening Form containing most of the KYC information together with other related forms filled in and documents provided by the customer during the account opening procedure shall be kept as a record of customer information collection.

The client risk profile assessment shall be recorded using Customer risk ranking tool and saving a pdf-printed copy of the results as well as other methods of customer risk assessment and documenting the conclusions of the assessor.

All customer identification records and any records made in respect of the verification process must be retained **for six years** after the closure of the customer account.

17. Requests for additional information from customers

If XFLOW determines that a prospective (or existing) customer has information that is likely to assist it in assessing, mitigating and managing its ML/TF risk, then XFLOW will provide notice to the prospective (or existing) customer requesting that information from them in accordance with SVG Law.

For example, a corporate customer may have a complex business structure for which the identification of the underlying beneficial owner is not readily identifiable. In this situation, requests will be made to the customer requesting clarity as to the structure.

18. Authorised service providers and official source electronic data

XFLOW considers that data obtained from recognized government sources (or those of an equivalent regulatory standing) is reliable and independent and thus, a suitable electronic data source to be used for verification purposes.

XFLOW has determined that it will also accept electronic data available from authorised service providers (commercial carriers) provided the following criteria are met:

(1) The carrier is authorised to store personal data;

(2) The carrier uses a range of information sources that can be called upon to link an applicant to both current and previous circumstances;

(3) The carrier accesses negative information sources, such as databases relating to identity fraud and deceased persons;

(4) The carrier accesses a wide range of alert data sources; and

(5) The process is transparent i.e. it is clear what checks were carried out, details of the results and the level of certainty as to the identity of the prospective customer.