CRISS FINANCIAL LIMITED

POLICY ON KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML)

Version Control

Sl. No	Version	Approved on	Approved by
1	Ver.1	22.05.2021	Board
2	Ver.2	28.04.2023	Board
3	Ver 3	31.07.2024	Board

1. INTRODUCTION:

Criss Financial Limited (herein after referred to as "Company" or "CFL") is registered as Non-Banking Financial Company with Reserve Bank of India (RBI)

In accordance with Master Direction issued by Reserve Bank of India vide DBR. AML. BC. No. 81/14.01.001/2015-16 on Master Direction - Know Your Customer (KYC) Direction, 2016 dated February 25, 2016 updated from time to time, all Non- Banking Financial Companies shall adopt and follow Know Your Customer (KYC) Policy and Anti Money Laundering (AML) Standards.

This Policy is applicable to various stakeholders including employees and customers of the Company.

2. OBJECTIVE:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering and financial terrorism activities. To educate the employees about the applicability of regulatory guidelines and the responsibilities to be performed by them to enable them to know/understand the customers and their financial dealings better, which in turn shall help in managing the risks prudently.

3. DEFINITIONS

(i) "Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

(ii) "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

(iii) "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

(iv) "Certified Copy" - Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the Act.

(v) "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a Customer.

(vi) "Customer "means.

a) A person or entity that maintains and/or has a business relationship with the Company;
b) One on whose behalf such relationship is maintained (i.e. the beneficial owner);
c) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and;
d) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company say a wire transfer or issue of a high value demand draft as a single transaction.

(vii) "Digital KYC" has the meaning as defined under extant RBI Directions.

(viii) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

(ix) "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a Company.

(x) "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the Customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

(xi) "Officially Valid Documents" or "OVDs" means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address including such other amendments as may be made to RBI Directions, from time to time.

(xii) "Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

(xiii) "RBI Directions" means provisions which are applicable to the Company under RBI Master Directions – Know Your Customer Directions, 2016, or such other Circulars, Notifications or guidelines issued by RBI from time to time on KYC/AML requirements.

(xiv) "Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

(xv) "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

(xvi) "Principal Officer" means an officer nominated by the Company as mentioned in the RBI Directions.

(xvii) "Senior Management" Senior Management for the purpose of the Policy shall constitute Managing Director & Chief Executive Officer, Manager (KMP), Chief Operating Officer, Chief Compliance Officer, Chief Risk Officer, Chief Technology Officer/Chief Information Officer.

(xviii) "Suspicious transaction" means a "transaction" defined suspicious as mentioned in the RBI Directions.

4. KEY ELEMENTS OF THE POLICY

The Company shall frame its KYC Policy incorporating the following four key elements:

1. Customer Acceptance Policy
2. Customer Identification Procedures.
3. Monitoring of Transactions; and
4. Risk management.

4.1. CUSTOMER ACCEPTANCE POLICY (CAP):

While taking decision to grant any facilities to the Customers as well as during the continuation of any facilities the following Customer Acceptance Policy (CAP) norms and procedures will be followed by the Company.

a) No account will be opened in anonymous or fictitious/Benami name.

b) No account will be opened where the Company is unable to apply appropriate Customer Due Diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

c) No transaction or account based relationship is undertaken without following the Customer Due Diligence procedure.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

e) Optional/additional information is obtained with the explicit consent of the customer after the account is opened.

f) A Unique Customer Identification Code (UCIC) shall be allotted to the customers. The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant Customer of the

Company desires to open another account with the Company , there shall be no need for a fresh CDD exercise. CDD Procedure is followed for all the joint account holders, while opening a joint account.

g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

h) The Company will ensure that the circumstances in which, a customer is permitted to act on behalf of another person/entity (authorization), is clearly spelt out.

i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

k) Where an equivalent e-document is obtained from the Customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

4.2. CUSTOMER IDENTIFICATION PROCEDURE (CIP):

Customer identification involves identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information and will be performed in the following scenarios.

a) While establishing a business relationship.

b) Carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

c) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

d) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

e) When Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold to avoid reporting.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Company may, rely on customer due diligence done by a third party, subject to the conditions specified in RBI Directions. The list of documents and procedure to be followed while conducting the CDD for individual customers is provided in Annexure I.

4.3. MONITORING OF TRANSACTIONS:

Ongoing monitoring is an essential element of effective KYC/AML procedures. The Company can effectively control and reduce the risk, by having detailed understanding on customer, customers' business and risk profile, source of funds on the normal and reasonable activities of the customer so that the Company can track/ identify the transactions that falls outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client.

The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall particularly attract the attention of the Company.

The Company will ensure that its branches continue to maintain proper record of all cash transactions. The internal monitoring system shall have an inbuilt procedure for reporting such transactions and those suspicious fraud in nature to controlling/ head office. The Company shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling with FIU-IND in terms of the direction of the RBI/PMLA in respect of all products/ services.

4.4. RISK MANAGEMENT:

The Board of Directors of the Company should ensure that an effective KYC program is put in place through establishing appropriate procedures and ensuring their effective implementation. It covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company in consultation with the Board, has devised procedures for creating Risk Profiles of existing and new customers and applied various Anti Money Laundering measures to recognize the risks involved in a transaction, account or business relationship.

The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company ensures that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and report the standards accordingly. The compliance in this regard shall be put up by Internal Auditors before the Audit Committee of the Board on quarterly intervals.

For Risk Management, the Company shall have a risk-based approach which includes the following:

a) Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of CFL.
b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and

their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities shall also be factored in.

c) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

d) Periodic updation shall be carried out at least once in every two years, for high-risk Customers, once in every eight years for medium risk Customers and once in every ten years for low risk Customers as per the RBI direction updated from time to time.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

Although the prospective customers of the Company are from the lower economic strata of society and hence, they are treated as low-risk clients, the Company shall ensure overall compliance with RBI KYC/Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of CFL.

Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities shall also be factored in requirements. The Company shall ensure compliance with all provisions relating to Client Due Diligence as made applicable from time to time under regulatory provisions.

In cases where any of the customers are found to be Medium/High-Risk, including their relatives or the beneficial interests in their accounts are held by persons other than the customers themselves, then the Company shall carry out enhanced due diligence procedures prescribed under applicable RBI Directions to gather sufficient information including information on sources of fund of family members and the close relatives.

The Company has an ongoing employee training programs to ensure that the employees are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

5. Money Laundering and Terrorist Financing Risk Assessment by the Company:

a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc.

b) The assessment process is in consideration with all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing

the internal risk assessment, The Company also takes cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor shares with the Company from time to time.

c) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

d) The outcome of the exercise shall be placed to the Board on annual basis and shall be made available to the regulatory authorities as and when required.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and the Company has Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the effectiveness of the controls and enhance them if necessary.

6. CUSTOMER EDUCATION:

Implementation of KYC procedures requires the Company to demand certain information from customers which may be of a personal nature, or which have hitherto never been called for. These may lead to numerous queries from the customer towards the motive and purpose of collecting such information. The Company shall prepare specific literature/ pamphlets etc. to educate the customer about the objectives of the KYC program. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

7. DESIGNATED DIRECTOR

To ensure compliance with the obligations under the Act and Rules, the Company shall nominate a Director on their Boards as "designated Director". The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

8. APPOINTMENT OF PRINCIPAL OFFICER

The Company shall appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. He / She shall maintain close liaison with enforcement agencies, banks and any other institutions which are involved in the activities of controlling money laundering and Combating the Financing of Terrorism. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

9. RECORD MANAGEMENT:

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information. The Company shall,

a) Maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;

b) Preserve the records pertaining to the identification of the customers and their addresses obtained

while opening the account and during the course of business relationship, for at least five years after the business relationship is ended.

c) Make available the identification records and transaction data to the competent authorities upon request.

d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) The nature of the transactions.
(ii) The amount of the transaction and the currency in which it was denominated.
(iii) The date on which the transaction was conducted; and
(iv) The parties to the transaction.

f) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

10. PERIODIC REVIEW AND ASSESSMENT:

Internal Audit department shall periodically evaluate and assess adherence to the prescribed processes and procedures with respect to KYC/AML requirements, unusual and potentially suspicious activities covering financial transactions with customers and other third parties.

The internal audit department would also provide an independent evaluation of compliance with the applicable RBI Directions, Act, and the Rules. Internal Audit would verify the application of KYC/AML procedures at the branches during every Branch/Regional processing Centre audit and comment on the lapses observed in this regard.

The internal audit department may also take the help of external agencies, wherever required, to assess, monitor, evaluate the effectiveness on the KYC/AML controls put in place in the Company, with the prior approval of the Senior Management of the Company.

Compliance with regard to the KYC/AML procedure shall be put up before the Audit Committee on quarterly intervals.

11. CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS:

All the information collected from the Customers by the Company shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the Customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that

behalf. Information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Exception to the confidentiality of customer information shall be as under:

(i) Where disclosure is under compulsion of law.
(ii) Where there is a duty to the public to disclose.
(iii) The interest of the Company requires disclosure.
(iv) Where the disclosure is made with express or implied consent of the customer.

12. SHARING OF INFORMATION WITH CENTRAL KYC REGISTRY (CKYCR):

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be with the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) as notified by the Government of India.

Annexure 1 – KYC Documentation

Details	KYC Documents
Photograph	Live photograph of the Customer is obtained.
Collection of OVD	Minimum one certified copy of Officially Valid Documents (OVD) 1. Voter's Identity Card issued by the Election Commission of India 2. Passport 3. Driving Licence, 4. Proof of possession of Aadhaar number 5. Job card issued by NREGA duly signed by an officer of the State Government 6. Letter issued by the National Population Register containing details of name and address
PAN	Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962. **[Mandatory]**
Other documents	Any one of the following, if the Company is not satisfactory in the OVDs submitted by the customer. 1. Ration card 2. Letter from any recognized public authority 3. Electricity bill 4. Telephone bill 5. Bank account statement 6. Letter from employer (subject to satisfaction of the Company) 7. A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority. Any one document which provides customer information to the satisfaction of the Company shall suffice. Based on the nature of the customer or their loan requirements, such other documents shall be demanded by the Company and the same shall be circulated through internal circulars, SOPs, notes etc. from time to time.

Aadhaar Compliance	The Company may carry out Offline Verification of Customers if they are desirous of undergoing Aadhaar Offline Verification for identification purposes. No such offline verification shall be performed without obtaining the written consent of the Customer in the manner prescribed in the Aadhaar Regulations. Wherever Aadhaar details are collected, it shall be ensured that Customers have redacted or blacked out their Aadhaar numbers through appropriate means. The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification, when the Company is authorised by RBI to do such verification for establishing account-based relationship. And will be performed in line with RBI/UIDAI guidelines.
Digital KYC	The Company may carry out verification by capturing live photo of the Customer and OVD or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with latitude and longitude of the location where such live photo is being taken by the authorized officer of the Company in line with the RBI guidelines on digital KYC process.

Where the OVD furnished by the Customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
b) property or Municipal tax receipt.
c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings if they contain the address.
d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

****