This Know Your Customer ("KYC") and Anti-Money Laundering ("AML") Policy ("KYC/AML Policy") describes the KYC and AML requirements to access and use our website https://cryptogyani.com and mobile application (collectively "Platform"), operated under the trade name "CryptoGyani," which offers services of online trading of cryptocurrency by placing sale and/or purchase orders of Users on outside cryptocurrency exchanges.

Block Trade Private Limited, a limited liability partnership registered in India in accordance with the Limited Liability Partnership Act, 2008 (hence referred to as "Us," "We," or "CryptoGyani," manages and runs the Platform. You acknowledge and agree that the terms of this KYC/AML Policy constitute a legally binding contract between you and CryptoGyani.

Parts of this KYC/AML Policy may be changed, modified, added, or removed at any time without previous written notice in CryptoGyani's sole discretion. You are responsible for frequently reviewing the KYC/AML Policy for any modifications or adjustments. You will be deemed to have accepted this Policy and any amendments made thereto if you continue to use the Platform after the KYC/AML Policy has been modified. You thus acknowledge and accept that the Terms of Use and Privacy Policy also apply to this KYC/AML Policy.

By signing this document, you expressly agree that CryptoGyani may continuously monitor your actions on our platform and gather information about them for the purposes of our KYC/AML Policy.

1. Definitions

1.1 "Applicable Law" refers to any statute, law, regulation, ordinance, rule, judgement, order, decree, by-law, approval from the relevant authority, government resolution, order, directive, guideline, policy, requirement, or other governmental restriction in force in India. This includes, but is not limited to, the Prevention of Money Laundering Act 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules 2005 ("PML Rules"), and various other applicable laws

1.2 "Crypto(s)" are virtual digital assets that may be moved, stored, or traded electronically using the Platform and refer to a cryptographically protected digital representation of money or legal rights utilising distributed ledger technology, including but not limited to bitcoin (BTC) and ether (ETH).

1.3 Anyone using or accessing the Platform to trade in cryptocurrencies is referred to as a "customer," "user," or "you."

1.4 "Customer Due Diligence (CDD)" refers to the process of locating a customer and confirming their identification utilising records, information, or data from a trustworthy, independent source.

For the purposes of this definition, "Aadhaar Number" refers to an identification number as defined by the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. "Officially Valid Document/OVD" refers to a passport, a driver's licence, proof of possession of an Aadhaar Number, or a voter's identity card issued by the Election Commission of India.

1.5 "Person" refers to a resident who is an Indian citizen and older than eighteen (18) years old.

1.6 "Politically Exposed Persons" (PEPs) are those with the legal right to perform important public duties in a nation, such as state governors, members of parliament, military personnel, senior government and

judiciary executives, and leaders of local organisations like municipal corporations. If you are a member of their family or a close relative of one, you may also be eligible to become a PEP.

1.7 A transaction, including an attempted transaction on the Platform, that, in CryptoGyani's sole discretion,: a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of a crime or an offence, regardless of the value involved; b. appears to have been made in circumstances of unusual or unjustified complexity or in violation of any Applicable Law; or c. appears to have no economic justification, Terrorism includes transactions involving funds suspected to be linked or related to or to be used for terrorism, terrorist acts, or by a terrorist, terrorist organization, or those who finance or are attempting to finance terrorism.

1.8 "User Account" or "CryptoGyani Account" refers to the account set up on the Platform through which the User instructs CryptoGyani to carry out a cryptocurrency transaction.

2. KYC norms

2.1 KYC is the key principle for the identification of any individual opening and operating a User Account. KYC means to 'Know Your Customer' which is an effective way for an institution to confirm and thereby verify the authenticity of a customer.

2.2 The customer identification should entail verification on the basis of documents and information provided by the customer. The objectives of KYC are as under:

a. To ensure appropriate customer identification,
b. Monitor the transactions of a suspicious nature,
c. Satisfy that the proposed customer is not an undischarged insolvent,
d. Minimize frauds,
e. Avoid opening Benami accounts with fictitious names and addresses, and
f. Weed out undesirable customers.

3. Declarations and Obligations

3.1 Declarations and Disclosure of Information by CryptoGyani

3.1.1 At the time You open a CryptoGyani Account and opt to trade using the Platform, CryptoGyani shall endeavour to identify and verify Your identity. To this effect, CryptoGyani shall collect, and You, as the User shall provide, such documents and data, as requested by CryptoGyani from time to time, to establish and verify the identity of the User / for KYC purposes / to establish and verify the nature of any Suspicious Transaction undertaken on the Platform. All data provided by You for KYC, and customer identification purposes or information on the Suspicious Transaction, shall be true, correct, and up-to-date. CryptoGyani may also use/deploy various software and/or technology or other means, either directly or through its service providers/vendors to establish and verify Your identity and/or the documents/information provided by You. You hereby consent to any such identity verification and KYC checks.

3.1.2 The documents and data for KYC and customer identification purposes shall be requested from the User and shall be accessed and used by CryptoGyani as per this Policy, the Applicable Laws, and the Privacy Policy accessible at https://cryptogyani.com/privacy-policy/.

3.1.3 CryptoGyani shall endeavour to verify, either itself or through third-party vendors/service providers, the identity and address of the Users along with the other details and documents submitted by You as may be legally/operationally tenable, including but not limited to using the following methods:

a. PAN/e-PAN verification through government sources; or
b. Masked/Offline Aadhar/Proof of Possession of Aadhar under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or
c. Passport issued under the Passports Act, 1967; or
d. Verification of Voter ID card issued by the Election Commission of India; or

e. Any other document may be required by CryptoGyani from time to time.

You as the User, hereby agree to provide the required documents and information for KYC checks in a timely manner, to create and to continue using the User Account through which the You may give instructions on the Platform.

3.1.4 Your failure as a User, to provide the requisite KYC documents or any identification documents or information as requested by CryptoGyani, may hinder, or completely restrict Your use of the Platform and the related services to the User.

3.1.5 You acknowledge and agree that the foregoing list of documentation, verification, and information may be amended by CryptoGyani by way of a notification/intimation, in its sole discretion from time to time, without prior notice.

3.1.6 CryptoGyani reserves the right to examine or request additional information and documents to establish Your identity, and financial position, including sources of Your funds and/or details of the Crypto wallet to which You transferred / from where You received any Crypto, and You shall provide all assistance and cooperation in this regard. If You fail/refuse to comply with the requirements herein, CryptoGyani shall not allow You to create or operate the User Account or carry out Crypto transactions through the Platform.

3.1.7 You agree to provide such additional documents as may be required by CryptoGyani, to ensure compliance with any Applicable Laws or CryptoGyani's policies or a request from any law enforcement authorities immediately, upon receipt of a written request from CryptoGyani.

3.1.8 You further represent, warrant, and agree to provide true, correct, and complete KYC documents, information, and data to CryptoGyani / its delegates/agents/representatives.

3.1.9 Where any transaction or series of transactions undertaken by You are considered as Suspicious Transaction(s) at the sole discretion of CryptoGyani or CryptoGyani reasonably perceives that it is likely to involve proceeds of crime or be used towards any illegal activity, or in an event, if CryptoGyani receives requests/requisitions from any banking partner/ payment system provider or participant/ statutory/ regulatory/ supervisory/ law enforcement authority/enforcement authority ("Authorities"), CryptoGyani shall report all such Suspicious Transaction(s) to the Authorities, as well as use, retain and share Your personal data, documents, and information available with CryptoGyani with the Authorities, and block and freeze Your access to the Platform and Your CryptoGyani Account, and may also increase the future monitoring of such User Account. You as the User, hereby undertake and warrant to provide all assistance, support, and cooperation in this regard including additional documents to verify the identity or the details of the transaction.

3.1.10 CryptoGyani does not allow the opening of or keeping any anonymous User Accounts or creating any accounts under fictitious names or on behalf of other persons whose identity has not been disclosed, or cannot be verified, or more than one (1) account for a person.

3.2 Your Obligations

3.2.1 You agree to use the Platform only for lawful and legal purposes as per this KYC/AML Policy, as amended from time to time, and the Applicable Laws.

3.2.2 You shall not use the Platform for any illegal or unlawful or criminal or anti-national purposes or for financing any such activity under any circumstance whatsoever.

3.2.3 You shall not impersonate another person or misrepresent Yourself on the Platform Under any circumstance whatsoever.

3.2.4 You undertake and warrant not to indulge in any Benami transactions or any transactions that are in violation of any Applicable Laws, this Policy or any other policy or instruction as issued by CryptoGyani from time to time.

4. Customer Acceptance Policy (CAP)

4.1 Account Opening Procedures

4.1.1 Any Indian national resident can open a CryptoGyani Account with CryptoGyani and such CryptoGyani Account can only be accessed within the geographical territory and jurisdiction of India.

4.1.2 The User has to provide the following before his/ her CryptoGyani Account can be made operational:

a. Permanent Account Number (PAN) given by Income Tax Authorities,
b. Documents for identification and proof of residence (Aadhaar/Voter ID/Passport),
c. Live selfie from the camera.

Please note that post the account opening process, the User would be required to add and verify their bank account/UPI ID for making INR deposits/withdrawals.

4.1.3 The above documents/data would help to establish the identity of the person opening the account but would not be sufficient to prepare a profile of expected activities in the CryptoGyani Account. Towards this, the following additional details may need to be collected while opening the CryptoGyani Account:

d. Annual income,
e. Occupation,
f. If Politically Exposed Person (PEP),
g. Trading experience, and
h. Marital status.

4.1.4 The User's CryptoGyani Account will only be made operational for the User to avail of our services when such documents, information as mentioned above, or any other additional information as requested by CryptoGyani has been verified as per the satisfaction of CryptoGyani.

4.2 CryptoGyani shall maintain an audit trail of any upload/modification/download

4.3 Safeguard measures taken by CryptoGyani

4.3.1 Before registering a CryptoGyani Account, We on a reasonable efforts basis ensure that:

a. Such CryptoGyani Account is not under an anonymous or fictitious/benami name.
b. No CryptoGyani Account is made operational and the User is not allowed to avail our services in an event if we are unable to apply appropriate CDD measures, i.e. verify the User identity and/or obtain documents required or non-reliability of the documents/information furnished to CryptoGyani, either due to non-cooperation of the User or non-reliability of the documents/information furnished by the customer.
c. No account is opened or trades are executed without following CDD procedure.
d. The User's identity does not match with any person with a known criminal background or having any association/ relationship with banned entities/ persons such as individual terrorists or terrorist organizations etc.

4.3.2 Users are not permitted to act on behalf of another User and can only transact on CryptoGyani's platform on their own account, with their own funds, and for their own benefit. Users are not permitted to open any of the following:

e. an anonymous account;
f. an account under a fictitious name; or
g. an account on behalf of other persons whose identity is undisclosed or unverifiable.

4.3.3 CryptoGyani at its sole discretion may review the User's CryptoGyani Account and transactions for any Suspicious Transactions or in an event if CryptoGyani receives a request for the same from Authorities and based on CryptoGyani's judgment or instruction from Authorities such CryptoGyani Account may be suspended, frozen, blocked, disabled, or terminated.

4.3.4 CryptoGyani may, in its sole discretion, refuse to open any new accounts, suspend or terminate existing User Accounts after giving due notice, or refuse to process any transactions on the Platform if it is unable to ensure compliance with any of the aforementioned conditions, either due to non-cooperation by the User or due to the details provided by the User being found enlisted on any Sanctions Lists or unreliable or unverifiable to CryptoGyani's satisfaction.

4.3.5 *Requirements/obligations under international agreements & Communication from international agencies*: CryptoGyani shall reasonably ensure that it does not have any account in the name of individuals appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC), other watchlists and sanctions lists.

5. Customer Identification Procedure (CIP)

One of the objectives of the "KYC" and data/information collection norms being carried out by CryptoGyani is to ensure appropriate Customer Identification. Customer Identification means undertaking the process of CDD. CryptoGyani may need to obtain sufficient information necessary to establish, to its satisfaction, the identity of each User, whether regular or occasional and the purpose of the intended nature of the transaction being executed on/ through the Platform.

Customer Identification Procedure is carried out at different stages while the Platform is accessed by the User and is not limited to instances when:

a. Registering a CryptoGyani Account,
b. Periodic review of a CryptoGyani Account,
c. Any transaction is being executed by the User on the Platform, and/or
d. CryptoGyani has a doubt about the authenticity/veracity or the adequacy of the earlier obtained User Identification data.

5.1 User identification

Identification of a User is an important prerequisite for registering and opening a CryptoGyani Account. No CryptoGyani Account is allowed on the Platform unless verification and due diligence of said User is successfully completed by CryptoGyani.

5.1.1 What is Identity?

Identity generally means a set of attributes that together uniquely identify a 'natural' or a 'legal' person. The attributes which help in the unique identity of a 'natural' or 'legal' person are called identifiers. Identifiers are of two types: a.) Primary and b.) Secondary.

a. Primary Identifiers: Means and includes the name (in full), Date of Birth, PAN number, and Passport number/Voter Identity Card/Driving License as they help in uniquely establishing the identity of the person.
b. Secondary Identifiers: Includes address, location, Nationality, and other such identification, as they help further refine the identity. User identification does not start and end at the point of application but it is always an ongoing exercise.

5.1.2 What is Identification?

Identification is the act of establishing who a person is:

c. In the context of KYC, identification means establishing who a person purports to be.
d. This is done by recording the information provided by the User covering the elements of his identity (i.e. name, and the address at which they can be located).
e. For undertaking CDD, the following shall be obtained from an individual while establishing a relationship. The features to be verified and the documents to be obtained for establishing the identity of a person are as under:
    i. Permanent Account Number (PAN) or the equivalent e-PAN, and
    ii. Certified copy of an Officially Valid Document (OVD) or the equivalent e-document thereof containing the details of identity and address. “Officially Valid Document” (OVD) means i) the Passport, ii) Aadhaar card, iii) the Voter's Identity Card, iv) or any other document as required by CryptoGyani from time to time and in its sole discretion.

5.1.3 What is Verification?

Verification of identity is the process of proving whether a person actually is who they claim to be. In the context of KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom CryptoGyani does business. This is done by carrying out checks on the correctness of the information provided by the customer.

5.1.4 Process of video-KYC

In scenarios where the document provided by a User has some issues and cannot be validated using the automated solutions CryptoGyani has in place, a video-KYC might be required from the User to validate the identity and authenticity of the document/ information submitted by them. We would also use the video-KYC process while performing enhanced due diligence wherever required.

5.1.5 Periodic updation of KYC

Periodic updation of KYC of Users is performed at such intervals of time and using such processes/documents as decided by CryptoGyani at its sole discretion. A risk-based approach for periodic updation of KYC is to be adopted:

f. No change in KYC information: In case of no change in the KYC information, a self-declaration from the User in this regard shall be obtained through User's email id and mobile number registered with CryptoGyani.
g. Change in address: In case of a change only in the address details of the User, a self-declaration of the new address may be obtained from the User through the User's email id and mobile number registered with CryptoGyani along with valid proof to be submitted by the User for the change in such address.
h. Change in contact information like a phone number or email address: In case of a change in the contact details of the User, the User can reach out to CryptoGyani to get the details updated, along with valid proof of change and demonstrating ownership of the CryptoGyani Account for which the details are to be updated.

5.2 Types of CDD

There are 2 types of Customer Due Diligence (CDD) that can be used in accordance with the risk category of the customer.

5.2.1 Basic Due Diligence means the collection and verification of identity proof, address proof, and a photograph to establish the identity of the User. This is done on the basis of the documents and information submitted by the User.

5.2.1 Enhanced Due Diligence (EDD) means additional diligence measures undertaken over and above the Basic Due Diligence. Steps under EDD shall include but will not be limited to checking if a User falls under the category of Politically Exposed Persons (PEPs), or is associated with any terrorist activities/groups, monitoring the account activity of such users, etc.

CryptoGyani shall conduct Basic Due Diligence, EDD, or any other due diligence activity or measures which under its sole discretion and/ or under Applicable Laws is required for a User registering or using the Platform.

6. Anti-Money Laundering Standards

CryptoGyani is vigilant in the fight against money laundering and under its best judgment implements processes not allowing any person to use the Platform for money laundering and terrorist financing activities.

6.1 Steps taken to prevent Money-Laundering activities and Terrorist Financing
CryptoGyani has implemented steps as described below with an objective to prevent any money laundering activity and/or terrorist financing on the Platform. Such processes being implemented are exhaustive in nature and are subject to change as required under any Applicable Law and/or as per CryptoGyani's sole discretion.

CryptoGyani may perform ongoing monitoring for the below sample scenarios:

a. Deposits from multiple bank accounts or UPI IDs
b. Withdrawals to multiple bank accounts
c. Very frequent deposits or withdrawals
d. Deposits and withdrawals without performing any trades

7. Monitoring of Transactions - On-going Due Diligence

7.1 Monitoring and supervision of the CryptoGyani Account in the event of any suspicious activity is detected is essential.

7.2 As part of the ongoing due diligence process, CryptoGyani may monitor CryptoGyani Account activities undertaken by a User through the Platform to reasonably ensure that they are consistent with their knowledge of the User, its risk profile, and where necessary, the source of funds.

7.3 When there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained User identification data, CryptoGyani may review the due diligence measures including reverifying Your identity, and may request additional information. You, the User hereby confirm that You shall provide all such information, as and when requested by CryptoGyani.

7.4 Monitoring customer activity and transactions throughout the relationship helps us to know their customers, assess risk, and provide assurance that CryptoGyani is not being used for the purposes of financial crime. However, the extent of monitoring shall be aligned with the risk category of the customer. High-risk accounts have to be subjected to more intensified monitoring.

7.5 Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored, whereas on basis of monitoring activities conducted by CryptoGyani as described under this Policy, any CryptoGyani Account may be frozen or suspended / User access might be blocked or terminated as decided by CryptoGyani under its sole discretion:

a. Very high account turnover inconsistent with the size of the balance maintained.
b. Special attention should be paid to the complex, unusually large transactions and all unusual patterns, inconsistent with the normal and expected activity of the User, which have no apparent economic rationale or lawful purpose.

7.6 CryptoGyani may enable alerts when the transactions are inconsistent with risk categorization and the updated profile of the customers shall be put into use as a part of effective identification and reporting of suspicious transactions.

8. Contact & Compliance Officer

8.1 CryptoGyani has appointed a 'Principal / Compliance Officer' to ensure overall compliance with the obligations imposed herein and under any Applicable Laws. At present, our Compliance Officer is Mr. Abhimanyu Kumar who can be reached at cs-compliance@CryptoGyani.co

8.2 In case of any complaint or queries with respect to this Policy or to report any suspicious or illegal activity of a User within Your knowledge, You may write to us at cs-compliance@CryptoGyani.co.

9. Risk Management by Periodic Review

9.1 Identification of a customer is an important prerequisite for opening an account. Non-adherence to this may lead to risks e.g. frauds, money laundering, inadvertent overdrafts, and Benami/fictitious accounts.

9.2 Non-compliance of monitoring of the transactions exceeding the threshold limit and non-recording of the transactions may result in intentional splitting/structuring of transactions to evade taxes, money laundering, and financing of terrorist activities.

9.3 CryptoGyani may carry out 'Money Laundering (ML) and Terrorist Financing ('TF') Risk Assessment' periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk for Users, countries or geographic areas, and products, services, transactions, or delivery channels that is consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government.

9.4 CryptoGyani, as a best industry practice and under its sole discretion categorizes the Users under low, medium, and high-risk categories, based on the assessment and risk perception. CryptoGyani should prepare the profile of the customer which should contain information relating to the customer's identity, social/financial status, nature of the business activity, and risk categorization shall be undertaken based on these parameters.

9.5 All User Accounts should be periodically updated based on their risk category. Unless otherwise required under this Policy or under Applicable Law or for complying with any request of Authorities, at present, the periodicity of such updation should not be less than once in five (5) years in the case of low-risk category customers, and not less than once in two (2) years in case of high and medium risk categories. CryptoGyani reserves the right to change the above periodicity at any time and from time to time in its sole discretion.

9.6 While considering the customer's identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in. The customer profile will be a confidential document and details contained therein shall not be divulged for cross-selling or any purposes other than those specified in this KYC/AML Policy, Terms of Service, Privacy Policy, or any other policies of CryptoGyani made available on the Platform or otherwise informed to the User from time to time.

9.7 CryptoGyani may take a view on risk categorization of each customer into low, medium, and high-risk categories depending on their experience, expertise in profiling of the customer based on their understanding, judgment, assessment, and risk perception of the customer and not merely based on any group or class they belong to.

9.8 The risk assessment carried out by CryptoGyani shall:

a. be reasonably documented;
b. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
c. be kept up to date; and

d. be available to competent authorities and self-regulating bodies/Authorities, if and as required under Applicable Laws.

10. Internal Controls

10.1 Preservation of Record / Record Management

10.1.1 CryptoGyani shall reasonably ensure that all information received for the purpose of identification or due diligence is used by it in accordance with CryptoGyani's terms and conditions applicable. CryptoGyani shall also take necessary reasonable steps for maintenance, preservation, and reporting of User information per the internal policies and standard operating procedures of CryptoGyani.

10.1.2 In addition, the confidentiality, security, and protection against access, use, and disclosure (including publication or display) of all information of a User, collected or created by CryptoGyani shall be kept in accordance with Applicable Law.

10.1.3 CryptoGyani shall collect and maintain records, in the form of books or stored in a computer, of Your identity proof along with all documents and information provided by You and of all the transactions undertaken by You on the Platform, as required under the Applicable Laws/good industry practices.

10.1.4 CryptoGyani shall maintain and report to Authorities the records of:

a. the KYC details, documents, and data of all Users who open a User Account on the Platform;
b. the KYC details, documents, and data of all Users who undertake a transaction on the Platform; or
c. Your transactions on the Platform.

10.1.5 Notwithstanding anything to the contrary contained in the Terms of Use or Privacy Policy, any information obtained while undertaking the due diligence measures under this Policy or during registration/creation/ongoing due diligence of Your CryptoGyani Account shall be maintained for the duration of the account is operational, and for a period of 10 (ten) years from the date the CryptoGyani Account ceases to exist or such longer period as may be specified under any Applicable Law/Authority.

10.2 CryptoGyani shall make available the identification records and transaction data to the authorities upon request.

10.3 If CryptoGyani:

a. suspects transactions of being involved in ML or TF, or
b. doubts the adequacy or veracity of previously obtained identification data,

necessary steps will be taken to review the due diligence measures undertaken by CryptoGyani or the information obtained (on the purpose and intended nature of the business relationship) from the User.

10.4 Hiring of Employees

Adequate screening mechanisms as an integral part of their personnel recruitment/hiring process shall be put in place to ensure high standards and equal and fair opportunity when hiring employees.

10.5 Employee training

10.5.1 Employee training programs are put in place so that the members of concerned staff are adequately trained in KYC/AML/CFT policy. The focus of the training could be different for frontline staff, compliance staff, risk management staff, Audit staff, and staff dealing with new customers. The front desk staff is trained to handle issues arising from a lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies, regulations, and related issues also ensure its proper implementation. e-Learning modules have been introduced for increased awareness.

10.5.2 CryptoGyani may put in place policies and FAQs to answer any queries or questions of the Users and satisfy them while seeking information in furtherance of the Policy.

10.5.3 We have taken every effort to ensure that this Policy adheres to the applicable laws. The invalidity or unenforceability of any part of this Policy shall not prejudice or affect the validity or enforceability of the remainder of this Policy. This Policy does not apply to any information other than the information collected by CryptoGyani through the Platform.

Annex 1 – KYC-AML Standards – Dos and Don'ts

Dos:

1. Before opening any new account, it is ensured that the prospective account opener‘s identity does not match with any person with a known criminal background, and their name does not appear in the list of terrorist individuals/ organizations banned by the UN Security Council Sanction Committee as circulated by RBI.
2. All the copies of supporting documents given by the customer must be photos/images of the original documents.
3. PAN shall be verified from the verification facility of the issuing authority.
4. All transactions of suspicious nature should be monitored.
5. High-risk accounts are subject to intensive monitoring and special attention is paid to all complex, usually large transactions which have no economical/lawful purpose.
6. Based on the risk perception, every new customer should be categorized into low, medium or high risk for monitoring purposes. Risk profiles of customers should be reviewed periodically.
7. Periodical updation of KYC information of every customer (including photographs) should be done.

Don'ts:

1. Do not open any account in anonymous or fictitious / benami name(s).
2. Do not open an account where CryptoGyani is unable to apply appropriate Customer Due Diligence (CDD) measures either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
3. Do not open any account without PAN and an ID document (Passport/Aadhaar/Voter ID card).
4. Services should not be denied to the general public, especially to those who are financially or socially disadvantaged.
5. In the accounts where suspicious activity has been observed, no restrictions are put on the operations and it is ensured that there is no tipping off to the customers.

Annex 2 - Sample suspicious activities

1. False Identity: Identification documents were found to be forged during the customer verification process.
2. Account of persons under investigation: The customer was reported in the media for being under investigation.
3. Account of wanted criminal: The name of the account holder and additional criteria (Date of birth/Father‘s name/Nationality) was the same as a person on the watch list of UN, Interpol, etc.
4. The account used for cybercrime: Complaints of cybercrime were received against a customer.
5. The account used for referral fraud: The customer was found to be creating fake accounts to obtain referral awards for them.

6. Unexplained activity in account inconsistent with the expected activity: Transactions in account inconsistent with what would be expected from expected activity.