

CENTRAL KYC RECORDS REGISTRY

CKYC/2024/05

Date: November 20, 2024

To: All entities registered with Central KYC Records Registry (CKYCRR)

Dear Sir / Madam,

Sub: Unique IP Address Requirement for CKYCRR API Access

Central KYC Records Registry (CKYCRR) set up under Prevention of Money Laundering (Maintenance of Records Rules, 2005), is a Reporting Entity, substantially owned and controlled by the Central Government, and authorized by the Government to receive, store, safeguard and retrieve the KYC records in digital form of a client in such a manner and to perform such other functions as may be required under these Rules. **As per Rule 9A, the Registry shall make such records available online to Reporting Entities.**

As per Rule 9(1A) of PML Rules, every Reporting Entity shall within 10 days after the commencement of account-based relationship with the client, file the electronic copy of the client's KYC records with the Central KYC Records Registry.

As per Rule 9(1C), for the purpose of verification of identity of a client or on-going due diligence, the Reporting Entity shall seek the KYC Identifier from the client or retrieve the KYC Identifier, if available, from the Central KYC Records Registry and proceed to obtain KYC records online by using such KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless:

- (a) there is a change in the information of the client as existing in the records of Central KYC Records Registry; or
- (b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the respective Regulator; or
- (c) the validity period of the downloaded documents has lapsed; or

(d) the Reporting Entity considers it necessary to verify the identity or address (including current address) of the client as per the guidelines issued by the Regulator under sub-rule (14) or to perform enhanced due diligence or to build appropriate risk profile of the client.

As per Rule 9(1D), a Reporting Entity after obtaining additional or updated information from a client under sub-rule (1C), shall within seven days or within such period as may be notified by the Central Government furnish the updated information to the Central KYC Records Registry.

As per Rule 9(1F), a Reporting Entity shall not use the KYC records of a client obtained from the Central KYC Records Registry for purposes other than verifying the identity or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorized to do so by the client or by the Regulator or by the Director.

Further, as CKYCRR is a Protected System notified by Govt Of India, your kind attention is drawn to Section 70, IT Act 2000 which states that any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

The Reporting Entities have to first register on CKYCRR to access its database. On registration, the entities are issued an FI code along with two admin user IDs. The registered entities can access CKYCRR through three modes viz website, SFTP and API (Search & Download).

This is in reference to the API integration between Reporting Entities and CKYCRR. To ensure data security, each Reporting Entity using CKYCRR API must use a unique IP address. This means that no two reporting entities can share the same IP address for CKYCRR API access. Reporting entities are directed to not share their login credentials, digital signatures, and API public/private keys with third parties. Reporting entities are also directed to ensure that the data obtained from CKYCRR is stored securely with adequate cybersecurity checks and controls and data protection measures in place so that there is no unauthorised access to the KYC data at any point in time, including during the transition between CKYCRR to the end point at the reporting entities' end. It is pertinent to note that

third parties 'pass-through or temporary access to CKYCRR data is considered as an example of unauthorized access.

We urge you to take immediate action to review your current integration with CKYCRR and obtain a unique IP address for your Institution's CKYCRR API usage. Sharing IP addresses and non-adherence to the above directions are violations of security, and failure to comply may result in termination of CKYCRR API access. By 31 December 2024, IPs that are common to multiple reporting entities shall be blocked from accessing CKYCRR APIs.

Kindly review the IP addresses registered by your institution using the 'Upload Public Key' option available under the 'User Management' menu in the CKYCRR web application portal and confirm in writing that a unique IP address belonging to your Institution only has been provided for CKYCRR API usage.

For and on behalf of **Central KYC Records Registry**

Helpdesk Contact Details:

Email: helpdesk@ckycindia.in

Phone: 022 61102592 / 022 50623300