CONSULTATION PAPER ON THE PROPOSED MODIFICATION TO THE INTERNATIONAL FINANCIAL SERVICES CENTRES AUTHORITY (ANTI MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND KNOW YOUR CUSTOMER) GUIDELINES, 2022.

Objective

The objective of this consultation paper is to seek public comments/ views on the proposed modifications to the Part-A of Annexure II ['Video based Customer Identification Process ('V-CIP') for Indian Nationals'] of the International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 ('Guidelines').

Statement of Object and Reasons

These draft modifications to the Guidelines aim to enable V-CIP for onboarding of Non-Resident Indians (NRIs) by the Regulated Entities.

Background

(1) The International Financial Services Centres Authority (IFSCA) was established under the International Financial Services Centres Authority Act, 2019 (IFSCA, Act) to develop and regulate financial products, financial services, and financial institutions in the International Financial Services Centres (IFSCs) in India.

(2) Pursuant to Section 12 & 13 of the IFSCA, Act and Rule 9 (14) of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ('Rules'), International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 ('Guidelines') were issued vide gazette notification IFSCA/2022-23/GN/GL001 dated October 28, 2022.

(3) The Guidelines currently permit Regulated Entities to onboard resident Indian nationals through V-CIP as specified under Part-A of Annexure-II. However, the existing

framework restricts connections from IP addresses outside India or spoofed IP addresses. This restriction, while aligned with security and compliance objectives, has posed a significant challenge for IFSC entities in onboarding Non-Resident Indian ('NRI') customers.

(4) In order to address the above issue, a working group was formed for the *"Development of Non-Resident Individual Business and Ease of Registration"* wherein one of the terms of reference of the Working Group was to suggest measures for the Ease of Registration of NRIs, including physical and digital onboarding, and related processes from the ease of investing through IFSC in India and Overseas. The Working Group conducted several discussions with stakeholders in IFSC and overseas jurisdictions and recommended allowing V-CIP for onboarding NRI customers.

(5) Considering the recommendations made by the working group, IFSCA proposes to modify the Guidelines to allow V-CIP for onboarding NRI customers from certain jurisdictions, supplemented with additional checks.

(6) In the initial phase, the Authority intends to enable the onboarding of NRI's categorized as low-risk customers and having proof of current address from certain jurisdictions such as United States of America, Japan, UAE, South Korea, etc. The consultation paper seeks feedback on the proposed V-CIP for NRIs, including suggestions for alternative modalities that could enhance the process. It also aims to identify potential challenges in implementing the V-CIP and explore ways to address them.

Public Comments

---

(1) In view of the above, comments and suggestions from public are invited on the draft modification to Part -A of Annexure II of the IFSCA (AML, CFT and KYC) Guidelines, 2022 contained in **Annexe**. The comments may be sent by email to Division of AML & CFT at aml-cft-div@ifsca.gov.in with the subject line "Comments on draft modification to Part -A of Annexure II of the IFSCA (AML, CFT and KYC) Guidelines, 2022" on or before **August 01, 2025**. The draft of the said Annexure is placed on the website of the IFSCA at https://ifsca.gov.in/ReportPublication/index/sKCVtbX6J9o=. The comments

may be provided in MS Word or MS Excel format only.

(2) The comments should be provided in the following format:

Name and Designation				
Contact No. and Email address				
Name of Organisation				
S. No.	**Clause no.**	**Text of the clause/ sub-clause**	**Comments/ Suggestions/ Suggested modifications**	**Detailed Rationale**

July 10, 2025
Gandhinagar

Annexe

Part-A of Annexure II ['Video based Customer Identification Process ('V-CIP') for Indian Nationals'] of the International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 ('Guidelines').

V-CIP FOR ONBOARDING INDIAN NATIONALS

1.1. Regulated Entities may undertake V-CIP to carry out:

(a) CDD in case of on-boarding of new customers such as an individual, proprietor (in case of a proprietorship firm), authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer.

(b) Updation/Periodic updation of KYC for eligible customers.

1.2. Regulated Entities opting to undertake V-CIP shall adhere to the following minimum standards:

1.2.1.V-CIP Infrastructure

(i) A Regulated Entity shall comply with the minimum baseline cyber security and resilience framework, as may be specified by the Authority, and all applicable laws on mitigating or managing Information Technology risks.
(ii) The technology infrastructure for V-CIP shall be housed within the premises of the Regulated Entity or its Financial Group; and the connections and interactions for undertaking V-CIP shall originate from its own secured network domain.
(iii) Any technology related outsourcing for the process shall be compliant with the standards, as may be specified by the Authority.
(iv) Where cloud deployment model is used, the Regulated Entity shall ensure that the ownership of data in such model rests only with the Regulated Entity or its Financial Group.

(v) Further, the Regulated Entity shall also ensure that all such data including video recordings are transferred to the server(s)/cloud server owned or taken on lease by the Regulated Entity or its Financial Group, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Regulated Entity.

Explanations:

Explanation I : In case the technology infrastructure is housed outside India with the Financial Group, the Regulated Entity shall immediately inform the Authority;

Explanation II : In case the data, including video recordings, are transferred to the server(s) or cloud server owned or taken on lease by the Regulated Entity's Financial Group, the Regulated Entity shall have access to such data.

(vi) A Regulated Entity shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application/digital platform, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(vii) The V-CIP infrastructure/application should be capable of preventing the connections from spoofed IP addresses.

Explanation. – For removal of doubt, it is hereby clarified that for resident customers, the IP address shall emanate from India and for residents of other countries from the country of United States of America, Japan, South Korea, United Kingdom excluding British Overseas Territories, France, Germany, Canada, UAE and Singapore.

(viii) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(ix) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Regulated Entity. Appropriate artificial intelligence (AI) technology with randomness and anti-deep fake and anti-fraud checks must be used to ensure that the V-CIP is robust.

(x) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

(xi) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration Testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In) or any such other suitably accredited agencies as may be specified. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(xii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

1.2.2.V-CIP Procedure

(i) Each Regulated Entity shall formulate a clear policy, workflow and standard operating procedure for V-CIP and ensure adherence to it.

(ii) The V-CIP process shall be operated only by officials of the Regulated Entity specially trained for this purpose. The official should be capable of carrying out liveliness check and detect deep-fakes, any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(iii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Regulated Entity. However, in case of call drop / disconnection, fresh session shall be initiated.

(iv) The sequence and/or type of questions, including those indicating the liveness of the interaction during video interactions shall be varied and randomised in order to establish that the interactions are real-time and not pre-recorded.

(v) Any prompting observed at the end of customer shall lead to rejection of the account opening process.

(vi) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.

(vii) The authorised official of the Regulated Entity performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

(a) Offline Verification of Aadhaar for identification;

(b) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer, or KYC Registration Agency (KRA) set up in IFSC;

(c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

(viii) A Regulated Entity shall redact or blackout the Aadhaar number in the manner as provided under Part B of Annexure II.

(ix) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

(x) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Regulated Entities shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document; if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Regulated Entities shall ensure that no incremental risk is added due to this.

(xi) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured as per the existing requirement. It shall be ensured

that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

(xii) A Regulated Entity shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified online from the database of the issuing authority including through Digilocker. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(xiii) The authorised official of the Regulated Entity shall ensure that photograph of the customer in the Aadhaar/ OVD and PAN/e-PAN, matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN, shall match with the details provided by the customer.

(xiv) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

(xv) All matters not specified under the above clauses but required under other statutes such as the Information Technology (IT) Act and the and the Digital Personal Data Protection Act, 2023 or the rules and regulations made thereunder, shall be appropriately complied with by the Regulated Entity.

1.2.3.V-CIP Records and Data Management

(i) The Regulated Entities shall ensure that the video recordings are stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in these Guidelines, shall also be applicable for V-CIP;

(ii) The activity logs along with the credentials of the authorised person of the Regulated Entity performing the V-CIP shall be preserved.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) Customers through V-CIP

(i) The Regulated Entities may onboard customers, who are Non- Resident Indian ('NRI Customers'), through V-CIP to carry out:

(a) CDD in case of on-boarding of new customers such as individual, proprietor in case of proprietorship, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer;

(b) Updation/Periodic updation of KYC.

Explanations. –

Explanation I: For the purposes of this part, the term "NRI customer" shall refer to a Non-Resident Indian who has been classified as a low-risk customer, by the Regulated Entity in accordance with these guidelines, and resides in any of the following jurisdictions:

a) United States of America;
b) Japan;
c) South Korea;
d) United Kingdom excluding British Overseas Territories;
e) France;
f) Germany;
g) Canada;
h) UAE;
i) Singapore.

Explanation II: For the avoidance of doubt, it is hereby clarified that the Regulated Entity shall undertake V-CIP only for NRI customers residing in any of the above specified jurisdictions and submits valid proof of current address to that effect.

(ii) While undertaking the V-CIP for onboarding the NRI customers, the Regulated Entity shall ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted to the Regulated Entities.

(iii) The Regulated Entities shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction specified in clause (i) above, for the purpose of verification of the current address.

(iv) Upon verification of the proof of identity of the NRI Customer, the Regulated Entity may open the account of the customer in the debit freeze mode; and shall communicate such customer the manner of activation of debit freeze account.

(v) The said debit freeze account of the NRI Customer shall be made operational only upon the receipt and verification of first credit from the bank account provided by such customer as proof of current address at the time of V-CIP onboarding process.

****