CIRCULAR F. No. -DAC/7/2024-AMLCFT 31st October, 2025 To All Regulated Entities in the International Financial Services Centres Subject: Modifications under the (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022. Sir/Madam, A. Reference is drawn to the (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 (hereinafter referred as 'Guidelines') issued vide notification /2022-23/GN/GL001 dated October 28, 2022. B. Pursuant to publication of consultation paper on this subject matter and comments/ suggestions received from the market participants and, on the examination, thereof, the hereby carries out the following modifications: (i) In clause 1.3.43. under the definition of Video based Customer Identification Process or V-CIP, after the words 'by an authorised official of the Regulated Entity,' and before the words 'by undertaking seamless, secure, live' the following words shall be added "or financial group entity in India supervised by a financial regulator or a KYC Registration Agency" (ii) Further the Part -A of Annexure II of the Guidelines shall be substituted as follows: - "PART-A V-CIP PROCESS 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 namely, "Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs" dated March 10, 2025 (as amended from time to time), issued by the Authority and all other 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 supervised by a financial regulator or a KYC Registration Agency (KRA); 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, using VPNs or proxy servers. Explanation. – For removal of doubt, it is hereby clarified that for resident Indian customers, the IP address shall emanate from India and for Non-Resident Indian it shall emanate either from India or from any one of the following countries where he or she is resident: 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; j) Australia. k) European Union excluding Croatia (viii) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp through use of tamperproof technology. 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, or financial group entity in India supervised by a financial regulator or a KRA Registration Agency under an agreement with specific terms and conditions ensuring customer secrecy and data protection. The Regulated Entity will be ultimately responsible for customer due diligence. (iii) The official should be specially trained for this purpose and capable of carrying out liveliness check and detect deep-fakes, any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs. (iv) 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. (v) 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 or by AI deep fake. (vi) Any prompting observed at the end of customer shall lead to rejection of the account opening process. (vii) 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. (viii) 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. (d) Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by RE. (ix) A Regulated Entity shall redact or blackout the Aadhaar number in the manner as provided under Part B of Annexure II. (x) 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. (xi) 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. (xii) 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. (xiii) 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 edocument including e-PAN is not valid for the V-CIP. Where a customer does not hold a PAN, an appropriate Form thereof shall be obtained. (xiv) 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/ePAN, shall match with the details provided by the customer. (xv) 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. (xvi) All matters not specified under the above clauses but required under other statutes such as the Information Technology (IT) Act 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 (classified as low-risk) 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; j) Australia; k) European Union excluding Croatia 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 Entity. (iii) The Regulated Entities shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction specified in Explanation 1 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." C. This Circular has been issued in exercise of the powers conferred under section 12 r/w 13 of the Act, 2019 and Rule 9(14) of the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005 and shall come into force with immediate effect. D. The number of jurisdictions from which V-CIP can be carried out has been restricted in the pilot phase of 4 months to certain countries. Addition of more countries will be considered once the pilot has been completed. E. Copy of the circular is available on the website at https://.gov.in/Legal/Index/TCce8MyOmco= Pradeep Deo, Chief General Manager Division of AML & CFT,