PUNE INTERNATIONAL CENTRE

Simplifying and Rationalising Security and Password Policies for Financial Institutions

With

Draft Regulatory Circulars for Consideration of the Reserve Bank of India (Annexure A) and the Securities and Exchange Board of India (Annexure B)

Umesh V. Kudalkar, CFA
Member, Pune International Centre (PIC)

August 2026

Submitted for the consideration of the Reserve Bank of India and the Securities and Exchange Board of India

Simplifying and Rationalising Security and Password Policies for Financial Institutions

With

Draft Regulatory Circulars for Consideration of the Reserve Bank of India (Annexure A) and the Securities and Exchange Board of India (Annexure B)

August 2026

Umesh V. Kudalkar, CFA
Member, Pune International Centre (PIC)

Submitted for the consideration of the Reserve Bank of India and the Securities and Exchange Board of India

Table of Contents

List of Abbreviations	
AAL	Authenticator Assurance Level
APIs	Application Programming Interfaces
CESG	Communications-Electronics Security Group
CPNI	Centre for the Protection of National Infrastructure
CSP	credential service provider
DPDP Act	Digital Personal Data Protection Act
IDRBT	Institute for Development and Research in Banking Technology
IBKR	Interactive Brokers
IBT	Internet Based Trading
KBA	knowledge-based authentication
Market-SOC	Market Security Operations Centre
MIRSD	Market Intermediaries Regulation and Supervision Department
NBFCs	Non-Banking Financial Companies
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSE	National Stock Exchange
PCI DSS	Payment Card Industry Data Security Standard
PIV/CAC	Personal Identity Verification or Common Access Card
RBI	Reserve Bank of India
RE	Regulated Entity
SEBI	Securities and Exchange Board of India
STWT	Securities Trading through Wireless Technology

Executive Summary

Consider two customers of two banks. Both banks are supervised by the Reserve Bank of India (RBI).

The first customer banks with Bank of Maharashtra. She must change her login password on a schedule. She cannot reuse any of her last five passwords. She keeps a second, separate transaction password under the same rules. She also maintains a four-digit PIN for the MahaSecure application, which the bank asks her to renew from time to time. That is three secrets to remember and renew, for one banking relationship.

The second customer banks with ICICI Bank. She has not been asked to change her internet banking password in more than twenty years.

Both banks follow the same Master Direction on Digital Payment Security Controls. Neither approach breaks any rule. Neither approach is required by any rule. But there is a gap between how the two banks follow the Master Direction. This paper is about closing that gap.

The technical question is settled. The U.S. National Institute of Standards and Technology (NIST) is the most widely followed authority on digital identity. On 31 July 2025, it published Revision 4 of its Digital Identity Guidelines. The relevant requirement reads: [1]

> *"Verifiers and CSPs SHALL NOT require subscribers to change passwords periodically. However, verifiers SHALL force a change if there is evidence that the authenticator has been compromised."*

Two terms need explaining. A **verifier** is the system that checks the password — for a bank, its own internet banking platform. A **CSP**, or credential service provider, is the party that issues and manages the credential. In NIST's drafting convention, "SHALL NOT" states a requirement, not advice. This is stricter than NIST's earlier position: the 2017 revision said only that verifiers "SHOULD NOT" require changes "arbitrarily (e.g., periodically)." Revision 4 raised it from a recommendation to a requirement. [2]

[1] NIST Special Publication 800-63B-4, *Digital Identity Guidelines: Authentication and Authenticator Management* (published 31 July 2025), Sec. 3.1.1.2 *Password Verifiers*, requirement 6: "Verifiers and CSPs SHALL NOT require subscribers to change passwords periodically. However, verifiers SHALL force a change if there is evidence that the authenticator has been compromised." pages.nist.gov/800-63-4/sp800-63b/authenticators. Publication record: csrc.nist.gov/pubs/sp/800/63/b/4/final.

[2] NIST SP 800-63B (Revision 3, 2017), Sec. 5.1.1.2, stated that verifiers "SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically)." Revision 4 raised this from a recommendation ("SHOULD NOT") to a requirement ("SHALL NOT") and replaced "memorised secret" with "password" throughout. csrc.nist.gov/pubs/sp/800/63/b/upd2/final.

Other authorities point the same way. Microsoft dropped the password-expiration setting from its recommended Windows security baseline in April 2019, describing periodic expiry as "an ancient and obsolete mitigation of very low value."[3] In the United Kingdom, CESG (the Communications-Electronics Security Group), the predecessor of the National Cyber Security Centre (NCSC), advised organisations not to enforce regular password expiry in September 2015, and the NCSC has kept that position since. [4]

The Reserve Bank has already begun this shift. Its (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025 were issued on 25 September 2025, with compliance required by 1 April 2026. For digital payment transactions other than card-present transactions, they require at least one factor that is dynamically generated and tied to the specific transaction, or capable of being proven, such as a biometric. [5] They do not deal with the login password itself, or with how often it must be changed. That is still left to each bank's own policy. This is why practice varies so widely.

This change is good for banks, not only for customers. Forced password changes generate reset requests, lockouts, call-centre volume and branch visits. All of these cost money. Removing them cuts that cost directly. It also removes one of the most common reasons customers find a bank difficult to deal with. Customers who abandon a session because they cannot recall which of six passwords they last used are customers who do not transact. A simpler login is a commercial gain as well as a customer-service gain.

Regulated entities should support this work. Banks and market intermediaries hold the data that will settle any remaining questions about Indian conditions. They should give that data to the Reserve Bank and to Securities and Exchange Board of India (SEBI) willingly and promptly. The

[3]A. Margosis, "Security baseline (DRAFT) for Windows 10 v1903 and Windows Server v1903," Microsoft Security Baselines Blog, 24 April 2019: "Periodic password expiration is an ancient and obsolete mitigation of very low value, and we don't believe it's worthwhile for our baseline to enforce any specific value." The setting was dropped from the recommended baseline; the capability was not removed from the operating system. learn.microsoft.com/.../security-baseline-draft-for-windows-10-v1903.

[4]CESG and CPNI, *Password Guidance: Simplifying Your Approach* (8 September 2015). CESG is the predecessor of the UK National Cyber Security Centre, which has maintained the position. assets.publishing.service.gov.uk/.../Password_guidance_-_simplifying_your_approach.pdf; NCSC, "The problems with forcing regular password expiry," ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry.

[5]Reserve Bank of India, *(Authentication Mechanisms for Digital Payment Transactions) Directions, 2025* (issued 25 September 2025; compliance required by 1 April 2026 unless otherwise specified). For digital payment transactions other than card-present transactions, at least one factor must be dynamically generated and uniquely tied to the transaction, or capable of being proven (for example, a biometric factor). Risk-based authentication is specifically required for cross-border card-not-present transactions. rbi.org.in/Scripts/NotificationUser.aspx?Id=12898.

change being asked for reduces their costs and improves their customer relationships. There is no good reason to slow it down.

Delay has a cost. Every month the present position continues; customers are put through a routine that the evidence does not support. They are pushed towards written-down passwords and reused passwords, which makes them less safe, not more. The change costs little, and it is reversible if a bank's own monitoring later shows a problem. ICICI Bank has operated without forced rotation for over two decades. The risk is manageable, and the method is already proven in the Indian market.

This paper sets out the evidence, four Indian case studies, and specific recommendations. It then gives both regulators complete draft circulars, at Annexure A and Annexure B, which they can issue for public comment substantially as drafted.

1. Why This Debate Matters

Password policy is one of the few parts of a bank's security design that every customer meets directly, and meets often. A badly designed policy does more than annoy people. It makes them less safe.

The reason is well documented. When customers are forced to change passwords often, they cope in predictable ways. They change one character at the end. They write the password on paper near the computer. They reuse the same password at several sites. NIST's own analysis makes the point concretely: a user who would have chosen "password" is relatively likely to choose "Password1" when required to add a capital letter and a digit. [6] Every one of these habits helps an attacker.

In India the problem is larger because of scale. A very large number of retail customers now bank online. As Section 5 shows, the rules they meet differ sharply from one RBI-regulated bank to the next. The strictness of a bank's password rules tells the customer nothing about how safe that bank actually is.

This paper does not ask for one rigid rule for every institution. It asks for Indian guidance to match the evidence-based approach that global standard-setters have already adopted. The prohibition on scheduled rotation is not made conditional, because the standard it follows is not conditional: NIST states the requirement as an unqualified "SHALL NOT." What the paper does add, as a parallel obligation on its own timetable, is that a bank must be able to detect a compromised password by better means. That obligation is at paragraph 53B of Annexure A.

[6] NIST SP 800-63B-4, Appendix A, *Strength of Passwords* (informative): "analyses of breached password databases reveal that the benefit of such rules is less significant than initially thought, and the impacts on usability and memorability are severe"; and "a user who might have chosen “password” as their password would be relatively likely to choose “Password1” if required to include an uppercase letter and a number." pages.nist.gov/800-63-4/sp800-63b/passwords.

2. The Evidence Has Changed: Global Standards No Longer Support Mandatory Rotation

For about twenty years, forced password changes were treated as obviously sensible. The idea was that a password changed often gives an attacker less time to use it. That idea did not survive testing. The bodies that once recommended rotation have since reversed their advice.

2.1 NIST SP 800-63B Revision 4 (July 2025) — The Global Reference Standard

NIST published Revision 4 of SP 800-63B on 31 July 2025. Because this paper relies on it heavily, the relevant requirements are quoted rather than summarised. They appear in Section 3.1.1.2, headed "Password Verifiers."

On periodic change (requirement 6): [7]

> *"Verifiers and CSPs SHALL NOT require subscribers to change passwords periodically. However, verifiers SHALL force a change if there is evidence that the authenticator has been compromised."*

On composition rules (requirement 5): [8]

> *"Verifiers and CSPs SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords."*

On password length (requirement 1): [9]

> *"Verifiers and CSPs SHALL require passwords that are used as a single-factor authentication mechanism to be a minimum of 15 characters in length. Verifiers and CSPs MAY allow passwords that are only used as part of multi-factor authentication processes to be shorter but SHALL require them to be a minimum of eight characters in length."*

[7] https://pages.nist.gov/800-63-4/sp800-63b/authenticators/ - passwordverhttps://csrc.nist.gov/pubs/sp/800/63/b/4/final NIST SP 800-63B-4, Sec. 3.1.1.2, requirement 6, quoted in full at n. 1 above.

[8] NIST SP 800-63B-4, Sec. 3.1.1.2, requirement 5: "Verifiers and CSPs SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords." Requirement 2 provides that verifiers and CSPs SHOULD permit a maximum password length of at least 64 characters; requirement 3 that they SHOULD accept all printing ASCII characters and the space character. pages.nist.gov/800-63-4/sp800-63b/authenticators.

[9] NIST SP 800-63B-4, Sec. 3.1.1.2, requirement 1: "Verifiers and CSPs SHALL require passwords that are used as a single-factor authentication mechanism to be a minimum of 15 characters in length. Verifiers and CSPs MAY allow passwords that are only used as part of multi-factor authentication processes to be shorter but SHALL require them to be a minimum of eight characters in length." pages.nist.gov/800-63-4/sp800-63b/authenticators.

The length requirement is quoted in full because it is easy to cite carelessly. NIST's fifteen-character minimum applies where the password is the only authentication factor. Where a password is used only as part of a multi-factor process, NIST requires a minimum of eight characters. The draft provisions at Annexure A therefore follow this distinction rather than imposing a higher minimum.

On screening against breached passwords: [10]

> *"When processing a request to establish or change a password, verifiers SHALL compare the prospective secret against a blocklist that contains known commonly used, expected, or compromised passwords."*

NIST adds a caution worth carrying into any Indian implementation: an excessively large blocklist gives little additional security benefit, because it defends against online guessing that is already limited by rate-limiting, while frustrating users trying to choose a memorable password.

On password managers: [11]

> *"Verifiers SHALL allow the use of password managers and autofill functionality. Verifiers SHOULD permit claimants to use the "paste" function when entering a password to facilitate password manager use when password autofill APIs are unavailable."*

This last requirement matters directly for Section 5.1.

2.2 PCI DSS 4.0.1 — Direction of Travel in the Payment Industry

Version 4.0.1 of the Payment Card Industry Data Security Standard (PCI DSS) was published in June 2024. Requirement 8.3.9 provides: [12]

> *"If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: Passwords/passphrases are changed at least once every 90 days, OR The security posture of accounts is*

[10]NIST SP 800-63B-4, Sec. 3.1.1.2: "When processing a request to establish or change a password, verifiers SHALL compare the prospective secret against a blocklist that contains known commonly used, expected, or compromised passwords." NIST adds that "[e]xcessively large blocklists are of little incremental security benefit." pages.nist.gov/800-63-4/sp800-63b/authenticators.
[11]NIST SP 800-63B-4, Sec. 3.1.1.2: "Verifiers SHALL allow the use of password managers and autofill functionality. Verifiers SHOULD permit claimants to use the "paste" function when entering a password to facilitate password manager use when password autofill APIs are unavailable." pages.nist.gov/800-63-4/sp800-63b/authenticators.
[12]https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1 PCI Security Standards Council, PCI Data Security Standard: Requirements and Testing Procedures, v4.0.1 (June 2024), Requirement 8.3.9: "If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: Passwords/passphrases are changed at least once every 90 days, OR The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly." The standard is available from the PCI SSC Document Library at pcisecuritystandards.org/document_library; publication was announced at blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1.

> *dynamically analyzed, and real-time access to resources is automatically determined accordingly."*

Two points of precision follow. First, the alternative to periodic change is dynamic analysis of account security posture — not any form of monitoring an institution chooses to call detection. The detection obligation proposed in this paper follows the same logic, though it is not framed as a condition of relief: unlike PCI DSS, NIST states the prohibition on periodic change without any alternative-compliance route. In this paper, paragraph 53B of Annexure A specifies what the detection capability must consist of.

Second, Requirement 8 governs personnel and third parties with access to the cardholder data environment. It is not intended to apply to the accounts of consumer cardholders. [13] PCI DSS is cited here as evidence of where the payments industry is heading, not as authority governing a bank's relationship with its retail customers.

Why the international standard refuses a conditional route. NIST could have written its rule the way PCI DSS writes Requirement 8.3.9 — no rotation, provided the institution can show something else instead. It did not, and the reasons matter for any Indian variant. A rule of the form "no rotation unless compromise is detected" is only as good as the detection behind it, and continuous monitoring for leaked credentials is difficult to operate reliably and fails silently rather than loudly; a conditional rule therefore makes the safety of every account depend on the weakest detection pipeline in the system. A conditional rule also invites inconsistent reading and uneven enforcement, which is precisely the condition Section 5 documents: four banks, one silent Master Direction, four different answers. An unqualified prohibition removes the guesswork. That is why this paper proposes detection capability as a parallel obligation with its own timetable, and not as the price a bank pays for relief.

2.3 Global Technology Industry and Government Practice

In April 2019, Microsoft removed the password-expiration setting from its recommended security baseline for Windows 10 v1903 and Windows Server v1903, on the basis that "periodic password

[13] https://pcidssguide.com/pci-dss-requirement-8/ PCI DSS v4.0.1, Requirement 8, applicability notes: the identification and authentication requirements of Requirement 8 are not intended to apply to accounts used by consumers (cardholders). The requirement governs personnel and third parties with access to the cardholder data environment. PCI SSC Document Library: pcisecuritystandards.org/document_library.

expiration is an ancient and obsolete mitigation of very low value." [14] Microsoft removed the recommendation, not the capability.

In the United Kingdom, government guidance has advised against forced expiry since September 2015, when CESG published Password Guidance: Simplifying Your Approach jointly with the Centre for the Protection of National Infrastructure (CPNI). CESG became the National Cyber Security Centre in 2016, and the NCSC has maintained the same advice. [15]

Login.gov is a programme[16] of the United States General Services Administration (GSA). It does not require periodic password changes. [17] One account lets users sign in to many government sites. As of October 2024, Login.gov had over 100 million accounts and 300 million-plus sign-ins a year[18]; it also lists 50-plus partner agencies. Login.gov requires multi-factor authentication (MFA) to create an account and sign in. Methods include an authentication app (e.g., Google Authenticator), a security key, a Personal Identity Verification or Common Access Card (PIV/CAC), face or touch unlock, text/call, or backup codes. [19] Login.gov does not force password changes on a schedule; users may change or reset a password anytime. Login.gov thus shows MFA can replace forced password rotation. The Trusted Traveler Programs of U.S. Customs and Border Protection (CBP) — Global Entry, NEXUS, SENTRI and FAST — use Login.gov to sign in. [20] CBP requires a second authentication step: an authentication application, a code sent by call or text, or a backup code. Login.gov lists Google Authenticator among the applications it supports.

[14] https://learn.microsoft.com/en-us/archive/blogs/secguide/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903 A. Margosis, Microsoft Security Baselines Blog, 24 April 2019, quoted at n. 3 above. learn.microsoft.com/…/security-baseline-draft-for-windows-10-v1903.

[15] https://assets.publishing.service.gov.uk/media/5a806bb9e5274a2e87db9b6a/Password_guidance_-_simplifying_your_approach.pdfhttps://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry CESG and CPNI, Password Guidance: Simplifying Your Approach (8 September 2015), cited at n. 4 above. ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry.

[16] Login.gov, "Frequently Asked Questions (FAQ): Is Login.gov a federal agency?": "Login.gov is not a standalone federal agency. We are a program of the General Services Administration (GSA) … run by the Technology Transformation Services (TTS)." login.gov/partners/faq. Accessed 2 August 2026.

[17] Login.gov, "How do I change my password?" The page describes only a user-initiated password change or reset, and does not describe a periodic password-change requirement. login.gov/help/manage-your-account/change-your-password. Accessed 2 August 2026.

[18] Login.gov, "Frequently Asked Questions (FAQ)": "As of October 2024, Login.gov has over 100 million user accounts with more than 300 million sign-ins annually." The same page separately reports over 50 partner agencies, a figure not dated to October 2024. login.gov/partners/faq. Accessed 2 August 2026.

[19] Login.gov, "Create an account" (multi-factor authentication is required to create an account): login.gov/help/create-account/overview; Login.gov, "Authentication methods": login.gov/help/create-account/authentication-methods; Login.gov, "Authentication application" (listing Google Authenticator): login.gov/…/authentication-application. All accessed 2 August 2026.

[20] Login.gov, "Trusted Traveler Programs (TTP)": login.gov/help/specific-agencies/trusted-traveler-programs; U.S. Customs and Border Protection, "Trusted Traveler Programs Application – Logging into Your Account": help.cbp.gov/s/article/Article-1456. Both accessed 2 August 2026. The CBP page describes a secondary authentication step (an application, a code sent by call or text, or a backup code) without naming a specific authenticator application.

Some will ask whether Indian retail customers are different. The behaviour that forced rotation produces is human, not national. People everywhere respond to forced changes by making small edits, writing passwords down and reusing them. What does differ between markets is the strength of a bank's fraud detection. That is what the parallel detection obligation in this paper addresses, at paragraph 53B of Annexure A. And India already has domestic evidence that the approach works, discussed at Section 5.2.

3. The RBI's 2025 Authentication Directions: A Major Step Forward — But Incomplete

The Reserve Bank issued the (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025 on 25 September 2025. Regulated entities must comply by 1 April 2026 unless otherwise specified. [21]

The Directions are a serious modernisation. For digital payment transactions other than card-present transactions, they require at least one authentication factor that is either dynamically generated and uniquely tied to that transaction, or capable of being proven — a biometric, for example. They also require risk-based authentication for cross-border card-not-present transactions specifically. The effect is to move the system beyond an assumption that an SMS one-time password is the answer in every case.

What they do not cover is the login password itself, and how often it must be changed. For banks, that remains governed by the Master Direction on Digital Payment Security Controls of 18 February 2021. [22] It is worth being precise about what that Master Direction actually says on the subject, because the paper's proposal builds on it directly.

Chapter III of the Master Direction deals with internet banking security controls. Paragraph 53, in full, provides: [23]

> *"Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login."*

The Master Direction abbreviates "Regulated Entity" as "RE" throughout; this paper otherwise spells the term in full. Two things follow. First, the Master Direction already regulates the life of a customer login password — it governs delivery, validity of a bank-issued password and a compulsory change at first login. Adding provisions on rotation and composition therefore extends

[21] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12898&Mode=0 Reserve Bank of India, (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, described at n. 5 above. rbi.org.in/Scripts/NotificationUser.aspx?Id=12898.

[22] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (RBI/2020-21/74, DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21, 18 February 2021). rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

[23] Master Direction on Digital Payment Security Controls, paragraph 53, in full: "Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login." rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

an existing subject rather than opening a new one. Second, and equally important, the Master Direction says nothing about how often a customer must change a password thereafter. That silence is the direct cause of the variation documented in Section 5. Bank of Maharashtra and ICICI Bank are both fully compliant with paragraph 53.

Two other instruments are relevant. [24] The Cyber Security Framework in Banks of 2 June 2016 sets baseline cyber-hygiene expectations but does not require or forbid rotation. [25] The Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices of 7 November 2023 deals with access controls at paragraph 19, but that paragraph governs need-based access to information assets and multi-factor authentication for privileged users. It is concerned with internal and privileged access, not with customer authentication.

This paper therefore proposes amending the Digital Payment Security Controls Master Direction, at Annexure A. Amending the Master Direction is preferable to a supervisory letter, because it is binding, public and clear to every bank at once.

[24] Reserve Bank of India, *Cyber Security Framework in Banks* (RBI/2015-16/418, DBS.CO/CSITE/BC.11/33.01.001/2015-16, 2 June 2016). rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1721.

[25] Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* (RBI/2023-24/107, 7 November 2023), paragraph 19 (Access Controls), which provides that access to information assets shall be allowed only where a valid business need exists, that personnel with elevated system access entitlements shall be closely supervised, and that REs shall adopt multi-factor authentication for privileged users of critical information systems. The paragraph governs internal and privileged access, not customer-facing authentication. rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12562.

4. Fraud Reality in India: What the Published Data Shows, and What It Does Not

Any proposal to remove a control must deal with the fraud data honestly, including the parts that complicate the argument.

4.1 RBI Annual Report 2024-25 — Understanding What Drives Fraud

The Reserve Bank's Annual Report 2024-25 records frauds reported by banks in FY 2024-25 totalling ₹36,014 crore, against ₹12,230 crore the previous year. [26] That headline figure is widely quoted, and widely quoted without the two qualifications that matter.

First, the number of cases fell. Reported fraud cases declined to 23,953 in FY 2024-25 from 36,060 in FY 2023-24. The amount rose while the count fell.

Second, the increase in amount is largely an accounting effect. The Reserve Bank attributed the rise principally to the reclassification of 122 previously reported cases, following the Supreme Court's judgment of 27 March 2023 in State Bank of India v. Rajesh Agarwal, which required banks to hear a borrower before classifying its account as fraudulent. [27] Those are large-value borrower accounts. They have nothing to do with retail internet banking passwords.

Stating the figure without these qualifications would invite the objection that retail digital fraud is exploding and this is no time to relax a control. The data does not support that reading.

What the data does show, and what is directly relevant, is the composition by number of cases. Card and internet frauds accounted for 13,516 cases, or about 56 per cent of all fraud cases reported in the year. This is the most frequent category, and it is the fraud the ordinary retail customer encounters. It deserves a serious response. The question is which response works.

One limitation must be acknowledged. The Reserve Bank's published aggregates do not break card and internet fraud down by root cause. They do not separate frauds involving a stolen or guessed password from frauds involving social engineering, malware or SIM swap. No published Indian

[26] https://www.rbi.org.in/Scripts/AnnualReportMainDisplay.aspx Reserve Bank of India, Annual Report 2024-25 (May 2025), Chapter on Regulation, Supervision and Financial Stability. Frauds reported by banks in FY 2024-25 totalled ₹36,014 crore by amount, against ₹12,230 crore in FY 2023-24, while the number of cases fell to 23,953 from 36,060. The increase in amount was attributed principally to the reclassification of 122 previously reported cases. Card and internet frauds numbered 13,516 cases. rbidocs.rbi.org.in — Annual Report 2024-25 (PDF); report index at rbi.org.in/Scripts/AnnualReportMainDisplay.aspx.

[27] The reclassification followed *State Bank of India & Ors v. Rajesh Agarwal & Ors*, Civil Appeal No. 7300 of 2022, judgment dated 27 March 2023, in which the Supreme Court held that the rule of *audi alteram partem* must be read into the RBI (Frauds Classification and Reporting by Commercial Banks and Select FIs) Directions, 2016, so that a borrower must be heard before its account is classified as fraudulent. The judgment concerns classification of borrower accounts, not customer liability for unauthorised electronic banking transactions. indiankanoon.org/doc/105925409/.

source known to the author provides that breakdown. Compiling it is one of the things the study recommended at paragraph 17 of Annexure A would deliver.

4.2 Social Engineering: A Large and Growing Share of Retail Digital Fraud

In the absence of an official root-cause breakdown, industry reporting is the best available evidence. It should be read for what it is: figures published by a commercial vendor, indicative of scale and direction rather than authoritative statistics. On that basis, BioCatch's reporting on Indian digital banking fraud records more than 100,000 "digital arrest" cases in 2024, a 146 per cent increase in text-message-based scams, and the detection of roughly 8.5 lakh mule accounts across more than 700 bank branches. [28]

The paper does not claim, and the available public evidence does not establish, that social engineering is a precisely quantified majority of Indian retail fraud by value. What the evidence does establish is that fraud of this kind operates at very large scale.

The consequence for password policy does not depend on the exact share. In each of these mechanisms the customer is induced to act: to approve a payment, to read out a one-time password, to install a remote-access application, or to let an account be used as a mule. A stronger password does not prevent any of them. A password changed last month does not prevent any of them.

This does not mean passwords do not matter. It means forced rotation is being asked to fight a threat it was never built to fight. Meanwhile the customer patience and bank resources it consumes are unavailable for the controls that do address that threat: transaction monitoring, callback verification and clear in-app warnings.

4.3 The Credential-Stuffing Exception

One credential-based threat is real and must be addressed. Credential stuffing is the automated use, at a bank, of username and password pairs leaked from unrelated websites. It works because people reuse passwords across sites.

[28] BioCatch, *Digital Banking Fraud Trends in India*, and associated press reporting: more than 100,000 "digital arrest" cases reported in 2024; a 146 per cent increase in text-message-based scams; and detection of approximately 8.5 lakh mule accounts across more than 700 branches of Indian banks. biocatch.com/report-digital-banking-fraud-trends-india-2025. These are figures published by a commercial vendor, cited as indicative of scale and not as official statistics.

This is precisely the risk NIST addresses through breach screening rather than rotation. [29] Checking a customer's password against lists of known compromised passwords catches the actual problem. Forced rotation was only ever a rough substitute for that check, and a poor one: it acts on a schedule rather than on evidence, and on every customer rather than the affected ones.

There is also a regulatory reason for banks to detect compromise properly. The Reserve Bank's customer protection framework of 6 July 2017 gives a customer zero liability for an unauthorised electronic banking transaction in two situations. The first is where the loss results from the bank's own negligence or deficiency. The second is a third-party breach, where the customer notifies the bank within three working days. The burden of proving customer negligence rests on the bank. [30] A bank that detects a compromised credential early protects its own balance sheet as well as its customer. This is why the detection obligation at paragraph 53B of Annexure A is built around demonstrated detection capability.

[29] https://pages.nist.gov/800-63-4/sp800-63b/authenticators/ - passwordver NIST SP 800-63B-4, Sec. 3.1.1.2, blocklist screening, quoted at n. 10 above.

[30] Reserve Bank of India, "Customer Protection — Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" (RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18, 6 July 2017). Zero liability applies where the loss arises from contributory fraud, negligence or deficiency on the part of the bank, and in third-party breach cases where the customer notifies the bank within three working days. The burden of proving customer negligence rests on the bank. rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336.

5. Comparative Case Studies: Indian Banks and Divergent Password Policies

Note on sources. This section is based on the author's own use of each bank's live retail platform as a customer. Dated screenshots of the Bank of Maharashtra login and password journey were captured between 13 and 15 April 2026 and are kept on file. [31] They are available to the Reserve Bank or to SEBI on request, and are not reproduced here only to keep this paper to a workable length. Where a bank's published terms do not themselves state a rule, the rule is described as observed in use, and is identified as such.

5.1 Bank of Maharashtra — The Most Restrictive Regime Observed

Bank of Maharashtra has the most demanding login and password regime among the banks reviewed. Before describing it, one point of fairness must be made, because it changes how the criticism should be framed.

Paragraph 51 of the Master Direction on Digital Payment Security Controls provides: [32]

> *"Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation ... Virtual keyboard option should be made available."*

So a captcha and an on-screen keyboard are not idiosyncrasies invented by the bank. They are responses to a requirement of the Master Direction, and the bank deserves credit for addressing it rather than criticism for having done so. The criticism that follows is therefore narrower and, being narrower, harder to answer: in three specific respects the bank's implementation does not do what paragraph 51 actually asks.

The observed features are these:

[31] The author's dated screenshots of the Bank of Maharashtra retail internet banking platform and of the MahaSecure application, captured between 13 and 15 April 2026, are retained on file and are available to the Reserve Bank of India or the Securities and Exchange Board of India on request.

[32] Master Direction on Digital Payment Security Controls, paragraph 51: "Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation ... Virtual keyboard option should be made available." rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

- Login is not available through an ordinary web browser. The customer must install and use the bank's own **MahaSecure** application from the app store.
- The MahaSecure app has its own four-digit PIN, separate from the login password and separate from the transaction password. On-screen prompts state that this PIN must be updated periodically. That is a third rotating secret for the same relationship.
- The User ID must be typed on an on-screen keypad rather than the device keyboard.
- Login also requires solving an arithmetic sum, such as "24 + 37 = ?", before the password is accepted.
- The login password must be changed periodically. The system also blocks reuse of any of the previous five passwords. In the author's experience this check once rejected a password that had not in fact been used recently.
- A separate transaction password authorises transfers, under the same composition rules and the same five-password history. The on-screen policy displayed at the point of change reads: "Password Length should be from 8 to 20 Characters. Password must start with Alphabet. Password can contain 1 to 19 Numbers, 1 to 19 Capitals, 1 to 19 Special Characters, 1 to 19 Alphabets. New password should not match with last 5 Passwords."
- A customer who forgets a password is directed to a branch visit or to knowledge-based security questions, which Section 9 addresses.

First, paragraph 51 is expressly risk-calibrated. It requires additional authentication "based on the RE's individual risk/ vulnerability assessment." It does not ask for a puzzle at every login by every customer regardless of any risk signal. An additional step triggered by an unrecognised device, an unusual location or a burst of failed attempts would satisfy the paragraph and would cost the ordinary customer nothing.

Second, the virtual keyboard is required to be an option, not the only method. Paragraph 51 says a "virtual keyboard option should be made available." Making it the sole means of entering a User ID goes beyond the requirement, and it is the specific feature that defeats password managers.

Third, an arithmetic sum is not a "strong CAPTCHA ... with anti-bot features." Simple arithmetic is trivially solved by an automated script, which is what a captcha exists to stop, while being genuinely difficult for a human to do quickly. The implementation is therefore weak against the

attack paragraph 51 is aimed at and burdensome for the customer it is not aimed at. A modern anti-bot challenge would be stronger and, for the great majority of customers, invisible.

Separately, the composition rule displayed on screen — a required mix of character types inside an eight-to-twenty character password — is the precise practice NIST's requirement 5 prohibits. And an application that does not work with password managers, combined with a mandatory on-screen keypad, runs against NIST's requirement that verifiers "SHALL allow the use of password managers and autofill functionality." [33]

The result is a regime built almost entirely on memorised secrets that must be rotated. There are three of them. Paragraph 53E of Annexure A responds to this pattern without disturbing paragraph 51: it does not stop a bank from requiring its own application or from deploying a captcha, but it requires the application to meet accessibility standards, to work with password managers, and to offer a non-branch alternative for customers who cannot use it.

5.2 ICICI Bank — A Working Model Already in Place

ICICI Bank sits at the other end of the range. The author's ICICI internet banking password has not been subject to any forced rotation requirement for more than twenty years. Login works through an ordinary web browser, without a mandatory proprietary application or an arithmetic puzzle.

This matters for three reasons.

First, it shows the policy works at Indian scale. ICICI Bank is a systemically important, RBI-supervised bank with a very large retail customer base. It has operated this way for over two decades, with no public indication of supervisory concern or unusual loss experience. Whatever doubts exist about applying international guidance to Indian conditions, this is Indian evidence, from an Indian bank, over a long period.

Second, it shifts the burden of justification. A control that a major Indian bank has done without for twenty years is not self-evidently necessary. Those who would impose it on every other bank should be asked to justify it.

Third, it gives the Reserve Bank a ready-made reference model. ICICI Bank has evidently not relied on forced rotation to manage credential risk, and must be relying on other controls instead. The Reserve Bank is uniquely placed to establish what those are, because it already receives the

[33] https://pages.nist.gov/800-63-4/sp800-63b/authenticators/ - passwordver NIST SP 800-63B-4, Sec. 3.1.1.2, password managers and autofill, quoted at n. 11 above.

supervisory data. If that data confirms that banks without forced rotation do not show higher fraud rates, the Reserve Bank should document how those banks manage the risk and publish it as a reference model. Other banks would then have a proven domestic template rather than a blank sheet. Paragraph 17 of Annexure A provides for this, and paragraph 53B lets a bank adopt the published model as its route to certification.

Fourth, the absence of a written commitment is not unique to ICICI Bank or to India. Retail password-rotation policy is generally not the kind of operational detail a bank states in writing for customers, whether in India or in markets with more developed disclosure practice. Informal enquiry suggests several major U.S. retail banks follow the same practice, though this paper does not independently verify it and does not rely on it. Silence on this point, in either market, is not evidence against the practice; if anything, it is closer to how the industry typically treats this particular parameter.

One qualification belongs here, because it is a real one. A password unchanged for twenty years has had twenty years in which it might have been exposed in a breach of an unrelated website and reused. That is the credential-stuffing risk described at Section 4.3. It is an argument for breach screening, which detects the exposure directly, and not an argument for scheduled rotation, which would not.

5.3 HDFC Bank and SBI — The Middle Ground

HDFC Bank and the State Bank of India sit in between. Both require periodic password changes, but at materially longer intervals than Bank of Maharashtra. Composition rules are less restrictive. Neither required a proprietary application for basic login in the author's experience. Both retain some password history restriction, shorter than five generations.

These two banks make the inconsistency point better than either extreme. There is no visible link between how strict each bank's rules are and any observable difference in customer risk or fraud exposure. The rules simply differ, and all four banks are compliant with the Master Direction as it stands. Paragraph 53C of Annexure A replaces this unexplained variation with one calibrated standard. Paragraph 53D(d) deals with a related practice found in this middle tier: printing a password on a statement that can be worked out from other details on the same statement.

5.4 Inconsistent Policies Within Financial Services Groups

The inconsistency also appears inside single financial groups. A group's bank and its broking or asset-management arm may share a brand and a customer base, yet apply very different password rules to what the customer experiences as one relationship.

This is not a criticism of either regulator. It follows from RBI-regulated and SEBI-regulated entities being governed by separate instruments written without reference to a shared customer. It is the main reason this paper submits parallel drafts to both regulators, at Annexure A and Annexure B, using matching structure and, so far as each statutory framework allows, matching standards. Paragraph 53F(d) of Annexure A addresses this alignment directly.

6. The Human Cost of Complex Password Policies

The friction described in Section 5 does not fall evenly. It falls hardest on the customers least able to absorb it: older customers, customers with limited digital experience, customers with weaker connectivity or older devices. Many of these customers are served by public sector and regional institutions, which often apply the stricter rules.

The costs are concrete. A customer who cannot do the arithmetic sum quickly cannot log in. A customer who has forgotten a security question set up years ago is locked out. A customer who must then travel to a branch loses a day's wages. A wealthier, urban customer of a bank with lighter rules faces none of this.

This is a fairness issue as much as a technical one, and it raises a scope problem the drafts must confront honestly. The Master Direction on Digital Payment Security Controls applies to Scheduled Commercial Banks excluding Regional Rural Banks, to Small Finance Banks, to Payments Banks and to credit card-issuing Non-Banking Financial Companies (NBFCs). [34] Regional Rural Banks, Urban Co-operative Banks and rural co-operative banks are outside it. A circular amending that Master Direction cannot reach them, however desirable that would be.

The drafts therefore do not pretend otherwise. Paragraph 21 of Annexure A does not purport to extend the circular to those institutions. It recommends instead that the Reserve Bank extend equivalent relief to them through the instruments that do apply to them, on the same basis and with a longer runway. It also provides that the detection requirement may be met through a sponsor bank, a federation, or a shared utility such as the Institute for Development and Research in Banking Technology (IDRBT). A reform that relieved only well-resourced banks, while leaving smaller institutions and their customers with the old burden, would not be a fair outcome. But saying so is not the same as being able to fix it in one instrument.

[34] Master Direction on Digital Payment Security Controls, paragraph 2 (Applicability): the Directions apply to Scheduled Commercial Banks excluding Regional Rural Banks, Small Finance Banks, Payments Banks, and credit card issuing NBFCs. Regional Rural Banks, Urban Co-operative Banks and State and Central Co-operative Banks are outside its scope, and cannot be brought within it by a circular amending it. rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

6.1 The Business Case for Banks

Removing forced password rotation is not a concession banks make to customers. It is in the banks' own interest.

- **It cuts direct costs.** Forced changes drive password resets, lockouts, call-centre calls and branch visits. Every one has a cost per incident. Removing the cause removes the cost. Paragraph 53I(b)(iii) of Annexure A asks banks to report that saving, so the industry can see the real numbers.
- **It increases usage and therefore business.** A customer who cannot remember which of six passwords is current often gives up on the session. Sessions abandoned at the login screen are transactions not made and products not bought.
- **It improves how banks are seen.** Complex, repetitive password rules are a common customer complaint. A bank that drops them, and explains that it has done so because the evidence supports it, looks modern and confident.
- **It supports digital adoption goals.** Every additional memorised secret works against bringing new customers into digital banking.
- **It frees resources for controls that work.** Money and staff attention spent administering rotation can be redirected to fraud monitoring and customer warnings, which address the threats Section 4.2 describes.

It follows that banks and market intermediaries should support this work rather than resist it. They hold the operational data that will answer any remaining questions about Indian conditions: reset volumes, lockout rates, login fraud by root cause, and outcomes under different password policies. They should provide it to the Reserve Bank and to SEBI promptly and in full. Paragraph 22 of Annexure A and clause 6.11 of Annexure B make this cooperation an express expectation.

7. Password Complexity Rules Often Reduce Security

A second common error is treating complexity as the same thing as strength. It is not.

A rule demanding one capital letter, one digit and one special character inside a short password narrows the field far more than it appears to. People satisfy such rules in the same few ways. NIST's own explanation is the clearest statement of the problem: a user who might have chosen "password" is relatively likely to choose "Password1" if required to include an uppercase letter and a number, or "Password1!" if a symbol is also required. [35] Attackers know this, because breached password databases show it.

This is why NIST's requirement 5 prohibits composition rules outright rather than merely discouraging them. [36]

Length is the more reliable protection, and it does not require the customer to guess what the system wants. A passphrase built from several unrelated words is easier to remember and much harder to guess. `Ladder7Compass$Harbor` is twenty-one characters drawn from three words and a connector. The strength comes from the words being chosen at random, not from them being real words.

This is the reasoning behind the length-first standard at paragraph 53C of Annexure A.

[35] https://pages.nist.gov/800-63-4/sp800-63b/passwords/ NIST SP 800-63B-4, Appendix A, Strength of Passwords (informative), quoted at n. 6 above.
[36] https://pages.nist.gov/800-63-4/sp800-63b/authenticators/ - passwordver NIST SP 800-63B-4, Sec. 3.1.1.2, requirement 5, quoted at n. 8 above.

8. Secure Credential Storage: A More Important Priority

If rotation is a weaker control than it appears, then what sits behind the login screen deserves more attention than it gets. A password is only as safe as the system storing it and the session it opens.

A long-lived session token is often a more attractive target than the password. Stealing it bypasses authentication entirely for as long as it lasts. Here the existing Master Direction has a gap that is easy to miss. Paragraph 52, in full, provides: [37]

> *"An online session shall be automatically terminated after a fixed period of inactivity."*

That is an inactivity timeout, and nothing more. A session that remains active is not caught by paragraph 52 at all. That is true whether the customer is genuinely using it, an attacker who has stolen the token is using it, or a script is generating activity to keep it alive. It may run indefinitely. There is no absolute cap on session duration anywhere in the Master Direction.

The substituted paragraph 52 at Annexure A closes exactly that gap. It keeps the inactivity rule and adds the second control the Master Direction lacks: an overall timeout that limits how long a session may run from the moment of authentication, irrespective of continued activity within it. NIST SP 800-63B Revision 4 requires both timeouts and sets the limits by assurance level. For a session at AAL2, which is the level retail internet banking with a second factor corresponds to, NIST states that the overall timeout should be no more than 24 hours and the inactivity timeout no more than one hour. Successful reauthentication during a session resets both. [38] It also prohibits renewing a session token without fresh authentication: NIST Sec. 5.1 provides that cookies and similar "remember my browser" features shall not be used instead of authentication.

On storage, NIST requires that passwords be salted and hashed using a suitable password hashing scheme, with a cost factor set as high as practical and raised over time as computing performance improves. Paragraph 53H of Annexure A gives that effect, and paragraph 53B makes detection capability the thing a bank certifies, rather than a policy statement.

[37] Master Direction on Digital Payment Security Controls, paragraph 52, in full: "An online session shall be automatically terminated after a fixed period of inactivity." rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

[38] Master Direction on Digital Payment Security Controls, paragraph 34(3): "multi factor authentication and alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits." Paragraph 33 requires multi-factor authentication for payments through electronic modes, with at least one factor being dynamic or non-replicable. rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

8.1 Breach Screening, Data Localisation and the DPDP Act

Breach screening means checking a customer's password against lists of passwords leaked in unrelated breaches. This raises an obvious data-handling question, which has a clear answer.

Done properly, screening never sends the customer's password anywhere. The standard method sends only a short prefix of a cryptographic hash. The service returns a large set of possible matches, and the comparison is completed inside the bank's own systems. This is a k-anonymity model. The full password and the customer's identity never leave the bank in any recoverable form.

[39] On that basis, breach screening involves no transfer of personal data under the Digital Personal Data Protection Act, 2023 (DPDP Act). [40] It also involves no transfer of payment system data under the Reserve Bank's directive of 6 April 2018 on storage of payment system data. The information compared is neither of those things.

Paragraph 53B(d) of Annexure A and clause 6.2 of Annexure B require this method, or an equivalent one offering the same guarantee.

[39]Digital Personal Data Protection Act, 2023 (No. 22 of 2023). meity.gov.in — Digital Personal Data Protection Act, 2023 (PDF).
[40]Reserve Bank of India, "Storage of Payment System Data" (DPSS.CO.OD.No. 2785/06.08.005/2017-18, 6 April 2018). rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

9. Passwordless and Risk-Based Authentication: The Future Direction

The longer-term direction is away from shared secrets altogether. Device-bound cryptographic credentials, known as passkeys, are already standardised. Biometrics tied to a registered device are widely deployed. Risk-based step-up authentication asks for more proof only when the context warrants it. The Reserve Bank's 2025 Directions point the same way, and so does paragraph 61 of the Master Direction, which invites regulated entities to consider alternatives to SMS-based one-time passwords where the second factor and the banking application sit on the same device. [41]

This paper's recommendations are an interim correction on the way to that destination.

The direction of travel is not confined to technology companies or general-purpose digital identity systems. Interactive Brokers (IBKR), a global financial-services and brokerage platform, had approximately 4.4 million institutional and individual brokerage customers worldwide as of 31 December 2025, and offers access to more than 170 electronic exchanges and market centres in 40 countries. [42] Its published security architecture provides a useful financial-services example of security controls being concentrated in stronger authentication and transaction safeguards. Interactive Brokers' Secure Login System provides an additional authentication factor alongside the username and password, protects customer cash and positions from unauthorised access, and provides higher withdrawal limits to customers using stronger authentication mechanisms. [43]

The author's own experience as an Interactive Brokers client provides a further practical illustration. The author uses the IBKR web portal as well as the IBKR Mobile application and has not been required to periodically change the account password. Instead, account access is protected through IB Key, Interactive Brokers' two-factor authentication mechanism integrated into the mobile application. When logging in through the web portal, the author receives a push notification on the iPhone and authorises the login through Face ID. Interactive Brokers' own documentation confirms that IB Key provides second-factor authentication through a push notification and

[41] Master Direction on Digital Payment Security Controls, paragraph 61: "Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms." rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

[42] https://investors.interactivebrokers.com/en/general/about/annual-report-and-proxy.php Interactive Brokers Group, Inc., Annual Report on Form 10-K for the fiscal year ended 31 December 2025 (filed 27 February 2026), Item 1 (Business): "Since the launching of our electronic brokerage business in 1993, we have grown to approximately 4.4 million institutional and individual brokerage customers"; the filing also records access to more than 170 electronic exchanges and market centres in 40 countries and 29 currencies. sec.gov — IBKR Form 10-K (FY2025).

[43] Interactive Brokers, Secure Login System – Strength and Security. The official documentation describes the additional authentication factor, protection of cash and positions, and enhanced daily and weekly withdrawal limits associated with stronger authentication.

requires facial recognition, Touch ID or a passcode to complete authentication. [44] The experience is therefore consistent with the principle this paper advances. A financial-services platform need not rely on calendar-driven password changes as its principal control. It can instead bind an additional authentication factor to the user's mobile device, and add transaction and withdrawal safeguards behind it.

This example is not presented as evidence that Interactive Brokers' entire security model can be transplanted wholesale into Indian retail banking. It is presented more narrowly. It is a real-world example from a large, internationally distributed financial-services platform, in which stronger authentication and transaction safeguards protect high-value financial assets — and in which the author has faced no periodic password-change requirement.

One practice should be corrected now: knowledge-based security questions — mother's maiden name, first school, and similar. NIST's requirement 8 provides: [45]

> *"Verifiers and CSPs SHALL NOT prompt subscribers to use knowledge-based authentication (KBA) (e.g., "What was the name of your first pet?") or security questions when choosing passwords."*

That requirement is directed specifically at the password-selection process: NIST does not permit verifiers to prompt subscribers to use knowledge-based authentication or security questions when choosing passwords. This paper extends that principle to account recovery as a matter of policy, not as a further NIST requirement: such questions are weak there for the same underlying reason, because their answers may be forgotten, reused or discoverable from public sources.

Practice bears this out. Section 5.1 shows the failure mode: the answer was set years ago and has been forgotten by the time it is needed, while the answers are often discoverable from public records or social media. Paragraph 53C(f) of Annexure A prohibits reliance on such questions as an authentication factor or as a sole means of account recovery, and clause 6.9 of Annexure B does the same for SEBI-regulated intermediaries.

[44] Interactive Brokers, IB Key – Two-Factor Authentication – iPhone. The official documentation describes the push-notification workflow and authentication using facial recognition, Touch ID or a passcode.

[45] NIST SP 800-63B-4, Sec. 3.1.1.2, requirement 8: "Verifiers and CSPs SHALL NOT prompt subscribers to use knowledge-based authentication (KBA) (e.g., "What was the name of your first pet?") or security questions when choosing passwords." Knowledge-based authentication is separately not among the authenticator types the publication permits at any assurance level. pages.nist.gov/800-63-4/sp800-63b/authenticators.

10. Recommendations

These recommendations combine two categories of change, and Annexures A and B identify each provision as it arises. Some directly implement NIST's core password requirements: no periodic rotation, no arbitrary composition rules, the fifteen/eight-character length distinction, blocklist screening at password establishment or change, and support for password managers and autofill. Others are additional design choices proposed for the Indian market — including the certification and screening mechanism at paragraph 53B, the minimum-attempt threshold at paragraph 53F, the account-recovery and phishing-resistant-authentication provisions at paragraphs 53J and 53K, and the notification, logging and reporting requirements at paragraphs 53G to 53I — that go beyond what NIST itself requires. The distinction matters because a reviewing regulator should be able to see clearly which obligations rest on the international standard and which rest on this paper's own policy judgment.

10.1 For the Reserve Bank of India

R1 — Verify the Indian position and publish a reference model. The Reserve Bank should compare fraud outcomes, by root cause, across banks with different password rotation policies, using supervisory data it already receives supplemented by data from banks. Two outputs matter. First, confirmation of what banks without forced rotation actually experience. Second, and more useful, a published description of how those banks manage credential risk instead — their breach detection, login monitoring and session controls. ICICI Bank's twenty-year record makes it the obvious starting point. Paragraph 17 of Annexure A provides for this on a twelve-month timetable. This work should run alongside the amendments below, not as a precondition to them.

R2 — Amend the Master Direction on Digital Payment Security Controls. The Reserve Bank should adopt the substituted paragraph 52 and the new paragraphs 53A to 53K at Annexure A. Their main effects are:

- An end to forced calendar-driven password changes, without making that relief conditional on a separate certification requirement.
- A NIST-aligned password standard at paragraph 53C, with a fifteen-character minimum where the password is used as a single-factor authentication mechanism and an eight-character minimum where it is used only as part of a multi-factor authentication process, replacing composition rules rather than adding to them. One can choose any combination of characters

as long as it meets the length requirement and is not found in a blocklist of compromised passwords. For a bank whose retail login remains single-factor, this raises the minimum from a typical eight characters to fifteen. A bank that requires a second factor at login falls under the eight-character rule instead, and by doing so also places itself outside the scope of PCI DSS Requirement 8.3.9. Merely offering, without requiring, a second factor leaves the password in single-factor use and does not qualify.

- Session management at paragraph 52 aligned with NIST SP 800-63B Revision 4, Section 5.2, including overall and inactivity timeouts determined with regard to the applicable authentication assurance level and session environment.
- Anti-enumeration and progressive-delay controls at paragraph 53F, supplementing paragraph 35 of the Master Direction, which requires a maximum number of failed attempts after which access is blocked but does not address enumeration or graduated response. [46]
- An end to formula-derived passwords printed on customer statements, at paragraph 53D(d).

A second factor at login is permitted and encouraged, not restricted. A bank that requires one moves its password to the eight-character standard and simultaneously places itself outside the scope of the only remaining international requirement for periodic rotation, PCI DSS Requirement 8.3.9, which applies where a password is the sole authentication factor. Where a second factor is already required at login, the password falls within the NIST multi-factor password-length provision, so multi-factor authentication strengthens authentication without requiring calendar-driven password rotation.

10.2 For SEBI-Regulated Entities

Annexure B extends a parallel standard to SEBI-regulated intermediaries under the Cybersecurity and Cyber Resilience Framework (CSCRF). [47] The CSCRF already classifies regulated entities into five tiers: Market Infrastructure Institutions, Qualified, Mid-size, Small-size and Self-certification. The draft is built around that structure rather than replacing it.

The securities market differs from banking in one respect that matters for the drafting. Login-level two-factor authentication is already mandatory for trading accounts. NSE Circular 36/2022 of 14

[46]Master Direction on Digital Payment Security Controls, paragraph 35: "REs should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. They should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts." rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

[47]Securities and Exchange Board of India, *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities* (SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, 20 August 2024). sebi.gov.in/legal/circulars/aug-2024/...-85964.html.

June 2022, issued in joint consultation with SEBI and the Exchanges under SEBI's Cyber Security and Cyber Resilience framework for Stockbrokers of 3 December 2018, requires members to use, in addition to a user ID, preferably biometric authentication together with a knowledge factor or a possession factor; where biometric authentication is not possible, both such factors must be used. The circular states that this "shall be implemented on every login session by the client to IBT (Internet Based Trading) and STWT (Securities Trading through Wireless Technology)." [48]

Two consequences follow. First, investor login is genuinely multi-factor, so NIST's eight-character minimum is the applicable reference point for the password used as part of that authentication process. The draft therefore adopts eight characters. Second, the trading workflow already has its authentication control, which is why the draft leaves it alone.

- A NIST-aligned password standard with an eight-character minimum for passwords used only as part of multi-factor authentication, at clause 6.3, applied consistently at login.
- An equivalent detection-capability requirement to that in Annexure A, at **clause 6.2**. Smaller intermediaries may meet it through a shared Market Security Operations Centre (Market-SOC) facility under **clause 6.2A**. The requirement does not apply until such a facility is available to them, and does not apply at all to intermediaries with no investor-facing platform.
- A closed list of actions needing a step-up factor beyond login, at **clause 6.8**: changing a payout bank account, changing a nominee, changing registered contact details, transferring or pledging holdings to a new demat account, and raising a limit. To be unambiguous: nothing in this draft requires a second factor to place, modify or cancel a trading order inside an authenticated session. The 2FA regime described above applies at login and is left undisturbed.
- A non-SMS second factor to be offered as an option rather than imposed as the only channel, at clause 6.8(c). This is consistent with the existing requirement that where an OTP is used it be sent by both email and SMS.
- An end to passwords on statements and contract notes derived from a guessable formula, at **clause 6.5**, mirroring paragraph 53D(d) of Annexure A.

[48]National Stock Exchange of India, Circular Ref. No. 36/2022, "Implementation of Two Factor Authentication" (Download Ref. No. NSE/COMP/52623, 14 June 2022), issued in joint consultation with SEBI and the Exchanges under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated 3 December 2018 on the Cyber Security and Cyber Resilience framework for Stockbrokers. Members must use, in addition to user ID, preferably biometric authentication together with a knowledge factor (password or PIN) or a possession factor (OTP, security token or authenticator application); where biometric authentication is not possible, both such factors must be used. The circular states that "the abovementioned authentication shall be implemented on every login session by the client to IBT and STWT," with effect from 30 September 2022. archives.nseindia.com/content/circulars/COMP52623.pdf.

- A prohibition on knowledge-based security questions, at **clause 6.9**, mirroring paragraph 53C(g) of Annexure A.

10.3 For Financial Institutions Generally

Institutions need not wait for either regulator to act. Four steps are available now, at low cost.

- **Publish the policy in plain language at account opening.** Customers should not discover the rules only when a change is forced on them.
- **Adopt length-first password rules now.** The case against complexity-for-its-own-sake rests on an express prohibition in the leading international reference standard.
- **Support password managers.** NIST requires verifiers to allow password managers and autofill, and recommends permitting paste into password fields where autofill APIs are unavailable. [49] Where a virtual keyboard is offered under paragraph 51 of the Master Direction, it should be an option rather than the only means of entry.
- **Verify email addresses before relying on them as trusted channels.** Existing onboarding processes may verify an email address through OTP, but legacy customer records may contain email addresses that were migrated to electronic communications without retrospective verification. A Regulated Entity should not use an unverified email address for OTP delivery or for transmission of confidential customer information. Where an email address has not been verified, the communication should instead be sent through another verified registered channel.
- **Cooperate with the regulators and share the data.** Institutions hold the reset volumes, lockout rates and fraud root-cause data that will settle the remaining questions.

[49] https://pages.nist.gov/800-63-4/sp800-63b/authenticators/ - passwordver NIST SP 800-63B-4, Sec. 3.1.1.2, password managers and autofill, quoted at n. 11 above.

11. Giving Effect to the Recommendations: The Draft Instruments at Annexures A and B

This paper does not stop at recommendations. Both regulators work more quickly from a draft than from prose. Annexure A is a complete draft circular amending the Master Direction on Digital Payment Security Controls. Annexure B is a complete draft circular amending the Cybersecurity and Cyber Resilience Framework.

Annexure A amends two things. Paragraph 52 on session management is replaced in full, for the reason given in Section 8. Eleven new paragraphs, 53A to 53K, are inserted after the existing paragraph 53, which is left untouched because it already deals correctly with password delivery and first-login change.

A note on the IT Governance Master Direction. An earlier version of this proposal also amended paragraph 19 of the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices. That amendment was meant to carry the accessibility and password-manager obligations. On examination that paragraph is not the right home. Paragraph 19 is headed "Access Controls," but it deals with need-based access to information assets, supervision of personnel holding elevated entitlements, and multi-factor authentication for privileged users. [50] It governs internal and privileged access, not the authentication of customers. Customer-facing accessibility and password-manager requirements belong in the Digital Payment Security Controls Master Direction, where Annexure A places them at paragraph 53E. No amendment to the IT Governance Master Direction is therefore proposed.

[51] One further drafting choice should be explained. The Cyber Security Framework in Banks of 2016 could have been the vehicle instead. Annexure A amends the Digital Payment Security Controls Master Direction because it is the more recent and more specifically payments-focused instrument, and because its Chapter III already deals with internet banking security controls, including the password provisions at paragraphs 51 to 53. If the Reserve Bank prefers the 2016 Framework, paragraphs 53A to 53K can be moved across without substantive change. Paragraph 23 of the draft allows for this.

[50] https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12562 Reserve Bank of India, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107, 7 November 2023), paragraph 19, discussed at n. 25 above. rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12562.

[51] https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1721 Reserve Bank of India, Cyber Security Framework in Banks (RBI/2015-16/418, 2 June 2016), cited at n. 24 above. rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1721.

11.1 Implementation Is Achievable Within a Reasonable Time

None of this is a large engineering programme. Most of it is straightforward, and one Indian bank (ICICI Bank) has been operating this way for over twenty years. The requirements fall into three groups.

Effective at T+3 months, at no material cost. Removing forced rotation, removing composition rules and ending formula-derived statement passwords are parameter changes in existing systems. They remove logic rather than add it, and can be made quickly.

Short-term configuration work. Session limits, anti-enumeration controls and customer notifications are standard features of modern banking platforms. Where a bank runs a third-party core platform, some may need a vendor release. The schedule at paragraph 12 of Annexure A and paragraph 10 of Annexure B allows for that, without holding up the immediate items.

Detection capability. This is the one genuinely new capability for banks that do not already have it. It is well-understood technology with established providers, and it is a capability banks should want regardless of this paper, because it addresses credential stuffing directly. A bank may adopt the reference model published under paragraph 17 rather than designing its own.

Two practical points remain. Dormant accounts cannot all be migrated by a single cut-over date without either intrusive customer contact or service disruption. Paragraph 53D(f) therefore migrates such credentials at the customer's next login, with invalidation only after thirty days' notice for credentials unused for twelve months. And on cost: implementing detection is not free, but the saving from fewer resets and lockouts runs the other way. Paragraph 53I(b)(iii) requires banks to report that saving, so the net position is visible rather than assumed.

11.2 Two Questions the Drafts Anticipate

Is a payments instrument the right vehicle? Login authentication is a precondition to every digital payment the Master Direction already governs, and the Master Direction already regulates the life of a login password at paragraph 53. [52] Paragraphs 53A to 53K extend an established category of regulation rather than creating a new one.

Is it right to add eleven new paragraphs to Chapter III? The relevant existing provisions are paragraphs 51 to 54. The new paragraphs are closely related and lettered as one family, 53A to

[52] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032 Master Direction on Digital Payment Security Controls, paragraph 53, quoted in full at n. 23 above. rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

53K, so they read as a single addition sitting behind the existing password provision. If the Reserve Bank prefers a different structure, paragraph 23 contemplates two alternatives: a free-standing circular incorporated by reference, or a new chapter dealing specifically with customer authentication. The substance does not depend on which is chosen.

Conclusion

One RBI-supervised bank (Bank of Maharashtra) requires a proprietary app, a third rotating PIN, an arithmetic puzzle and a five-password history. Another RBI-supervised bank (ICICI Bank) has not required the author, a customer of more than twenty years, to change a password in that time. The observed practices at both banks are not inconsistent with the Master Direction as it stands, because paragraph 53 is silent on periodic password changes. The leading international reference standard now prohibits, in mandatory terms, the practice the first bank follows.

The change proposed here is customer-friendly, cost-reducing and commercially sensible for the institutions that must implement it. A major Indian bank has operated without mandatory periodic password rotation for more than two decades, providing useful domestic evidence that the approach can be sustained at scale. The main risk now is not that the change goes wrong. It is that it takes years longer than it needs to, while customers continue writing passwords on paper because the rules leave them no better option.

This paper asks four things.

- **Issue the draft at Annexure A for public comment**, so that banks and consumer representatives can test the drafting.
- **Run the comparative study at paragraph 17 alongside it**, on a twelve-month timetable, and publish the resulting reference model so that banks have a proven Indian template to follow.
- **Take up the SEBI draft at Annexure B** in the next scheduled CSCRF review, so that a customer moving between a group's bank and its broking arm meets one coherent policy.
- **Encourage two steps that cost nothing and need no circular**: publishing password policy in plain language at account opening, and allowing password managers to work.

None of this asks anyone to be careless about compromised credentials. It asks that the care be aimed at the things that actually cause loss — credential stuffing, breach reuse and session theft — and that customers be relieved of a burden that does not.

References and Sources

Primary sources relied upon. Each source name links to the document cited. Where a proposition rests on a specific requirement, the locator column gives the pinpoint reference and the footnote in the text quotes the language relied upon.

Source	Locator relied upon	Publisher	Accessed
NIST SP 800-63B-4 (Rev. 4)	Sec. 3.1.1.2, requirements 1, 5, 6, 8; blocklist and password-manager provisions	NIST (pub. 31 Jul 2025)	Aug 2026
NIST SP 800-63B-4, Appendix A	Strength of Passwords (informative) — composition-rule research	NIST	Aug 2026
NIST SP 800-63B (Rev. 3, 2017)	Sec. 5.1.1.2 ("SHOULD NOT" — superseded by Rev. 4)	NIST	Aug 2026
Microsoft security baseline, Windows 10 v1903	A. Margosis, 24 Apr 2019 — removal of password-expiration setting	Microsoft	Aug 2026
CESG/CPNI, Password Guidance	Simplifying Your Approach (8 Sep 2015)	CESG (now NCSC), UK	Aug 2026
NCSC — problems with forcing regular password expiry	Continuing UK position	NCSC, UK	Aug 2026
PCI DSS v4.0.1	Requirement 8.3.9 (single-factor only)	PCI SSC (Jun 2024)	Aug 2026
PCI DSS Requirement 8 scope guidance	Scope excludes consumer cardholder accounts	PCI DSS Guide	Aug 2026
RBI Master Direction — Digital Payment Security Controls	Para 2 (applicability); paras 33–35; Chapter III paras 51, 52, 53; para 61 — all quoted verbatim in text	Reserve Bank of India	Aug 2026

Source	Locator relied upon	Publisher	Accessed
RBI Master Direction — IT Governance	Para 19 (Access Controls) — verified as governing internal/privileged access	Reserve Bank of India	Aug 2026
RBI (Authentication Mechanisms) Directions, 2025	Issued 25 Sep 2025; compliance by 1 Apr 2026	Reserve Bank of India	Aug 2026
RBI Cyber Security Framework in Banks (2016)	RBI/2015-16/418, 2 Jun 2016	Reserve Bank of India	Aug 2026
RBI Annual Report 2024-25	₹36,014 cr; 23,953 cases; 122 reclassified; card and internet frauds 13,516 (56.5%)	Reserve Bank of India	Aug 2026
SBI v. Rajesh Agarwal, Supreme Court of India	27 Mar 2023 — hearing before fraud classification; basis of the FY25 reclassification	Supreme Court of India	Aug 2026
RBI — Limiting Liability of Customers in Unauthorised Electronic Banking Transactions	RBI/2017-18/15, 6 Jul 2017 — zero liability; burden of proof on the bank	Reserve Bank of India	Aug 2026
SEBI CSCRF Circular	20 Aug 2024; five-tier RE classification	SEBI	Aug 2026
NSE Circular 36/2022 — Two-Factor Authentication	Ref. NSE/COMP/52623, 14 Jun 2022; 2FA on every login session to IBT and STWT; under SEBI/HO/MIRSD/CIR/PB/2018/147 of 3 Dec 2018	National Stock Exchange of India	Aug 2026

Source	Locator relied upon	Publisher	Accessed
Digital Personal Data Protection Act, 2023	No. 22 of 2023	Ministry of Electronics and IT	Aug 2026
RBI — Storage of Payment System Data	Localisation directive, 6 Apr 2018	Reserve Bank of India	Aug 2026
BioCatch — India digital banking fraud reporting	Digital-arrest case count; SMS scam increase; mule account detection	BioCatch (commercial)	Aug 2026

Standard of citation used in this paper. Where a requirement of a published instrument is relied upon, the paper quotes the operative words and identifies the party on whom the obligation falls. Every paragraph of the Master Direction on Digital Payment Security Controls referred to in Annexure A has been checked against the consolidated text on the Reserve Bank's website, and the paragraphs substituted or built upon — 51, 52 and 53 — are quoted in full in Sections 3, 5.1 and 8 so that a reader can verify the amendment against the existing provision without leaving the paper.

Author's direct evidence. The Bank of Maharashtra case study at Section 5.1 comes from the author's own use of that bank's retail internet banking and MahaSecure application. Dated screenshots captured between 13 and 15 April 2026 are kept on file and are available to the Reserve Bank or to SEBI on request. Observations on ICICI Bank, HDFC Bank and the State Bank of India rest on the same basis. None is presented as a statement sourced to, or endorsed by, either regulator.

Note on industry data. The BioCatch figures at Section 4.2 are published by a commercial fraud-analytics vendor and are cited as indicative of scale, not as official statistics or as the sole authority for any recommendation.

Annexure A — Draft Circular for Consideration of the Reserve Bank of India

Customer Login Authentication and Password Policy for Internet Banking

RBI/2026-27/[•] — DoS.CO.CSITE.SEC.No. [•]/31.01.015/2026-27 — [Draft for public comment]

To — All Scheduled Commercial Banks (excluding Regional Rural Banks); Small Finance Banks; Payments Banks; Credit Card-issuing NBFCs

Note on addressees. This list reproduces the applicability of the Master Direction on Digital Payment Security Controls, which this circular amends. Regional Rural Banks, Urban Co-operative Banks and rural co-operative banks are outside the Master Direction and cannot be brought within it by this circular; paragraph 21 addresses them separately.

Madam / Dear Sir,

Amendment to the Master Direction on Digital Payment Security Controls — Customer login authentication and password policy

A. Background

1. Please refer to the Master Direction on Digital Payment Security Controls (RBI/2020-21/74, DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21, dated 18 February 2021), as amended from time to time ("the Master Direction").

2. Paragraph 53 of the Master Direction presently governs the secure delivery of a login password, the limited validity of a password generated and dispatched by a Regulated Entity, and the requirement that the user change such a password compulsorily on first login. The Master Direction does not prescribe how frequently a customer must change a login password thereafter.

3. On a review of current practice, it is observed that customer login-password policy for retail internet and mobile banking varies materially between Regulated Entities in the absence of such a provision. This variation does not correspond to any demonstrated difference in customer risk profile.

4. It is further observed that the international standard-setting position on mandatory calendar-driven password rotation has changed since the Master Direction was issued. NIST Special Publication 800-63B-4, published on 31 July 2025, provides at Section 3.1.1.2 that verifiers and

credential service providers "SHALL NOT require subscribers to change passwords periodically," while requiring a change where there is evidence that the authenticator has been compromised. The same Section provides that verifiers and credential service providers "SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords," and that verifiers "SHALL allow the use of password managers and autofill functionality."

5. It is further observed that paragraph 52 of the Master Direction requires termination of an online session after a fixed period of inactivity, but does not limit the total duration of a session in which activity continues.

6. It is further observed that the (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, do not address login-password rotation, which accordingly remains governed by the Master Direction.

7. It is also observed that mandatory rotation imposes avoidable cost on customers and on Regulated Entities alike, in the form of password resets, account lockouts, call-centre volume and branch visits, without a corresponding security benefit. Removing it is expected to reduce operating cost, improve customer experience and support wider adoption of digital banking channels.

8. It is accordingly considered necessary to amend the Master Direction to (i) remove mandatory periodic password rotation, (ii) require demonstrated compromise-detection capability as a separate and parallel obligation, (iii) prescribe a length-first password standard in place of composition rules, and (iv) address related session-management, anti-enumeration, accessibility and reporting matters.

9. In exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934, and the Payment and Settlement Systems Act, 2007, the Reserve Bank of India hereby amends the Master Direction as follows.

B. Amendments

10. In Chapter III of the Master Direction, for paragraph 52, the following shall be substituted, namely:

"52. Session management. — (a) An online session shall be automatically terminated after a fixed period of inactivity. (b) Overall and inactivity timeout limits for authenticated sessions shall be established in accordance with NIST SP 800-63B Revision 4, Section 5.2, read with Sections 2.1.3, 2.2.3 and 2.3.3. The applicable limits shall take into account the authentication assurance level, the environment in which the session is conducted, the type of endpoint being used, whether the endpoint is a managed device, and the nature of the application. (c) A session may be extended through a reauthentication event in accordance with that Section. (d) When either timeout expires, the session shall be terminated. (e) A session token shall not be renewed or extended without a fresh authentication event, and a persistent 'remember this browser' facility shall not be used in place of authentication."

Drafting note. Sub-paragraph (a) preserves the existing paragraph 52 without change. Sub-paragraphs (b) to (e) align session management with NIST SP 800-63B Revision 4, Section 5.2, which provides for overall and inactivity timeouts and states that their limits depend on the authentication assurance level, session environment, endpoint, whether the endpoint is managed, and the nature of the application.

11. In Chapter III of the Master Direction, after paragraph 53, the following paragraphs shall be inserted, namely:

"53A. No mandatory periodic password change. — A Regulated Entity shall not require a retail customer to change an internet or mobile banking login password on a fixed calendar schedule. A change may be required where the customer has been notified of, or the Regulated Entity has reason to believe there has been, a compromise of the password. Nothing in this paragraph affects the requirement in paragraph 53 that a password generated and dispatched by the Regulated Entity be changed on first login."

"53B. Detection capability. — (a) A Regulated Entity shall certify to the Reserve Bank, in the manner it may specify, that it has implemented a compromise-detection methodology including, at minimum: (i) screening a password against corpora of known-compromised credentials when the password is established or changed, and re-screening the password each time it is submitted at login, before it is accepted, against the same corpora; and (ii)

monitoring for anomalous login behaviour indicative of credential-stuffing or account-takeover activity.

(b) A Regulated Entity may satisfy sub-paragraph (a) by adopting the reference model published by the Reserve Bank under paragraph 17. A Regulated Entity that does so is not required to design an independent methodology.

(c) A Regulated Entity shall submit its implementation plan by T+2 months and complete implementation by T+9 months, "T" being the date of commencement of this circular. The requirements in paragraph 53A shall apply according to the implementation timeline in paragraph 12. The Reserve Bank may, on application showing genuine third-party vendor dependency, extend this date by up to six months for a specific entity.

(d) The screening required by sub-paragraph (a)(i) shall not involve the transfer of any customer password or personal data to a third party in reversible or identifiable form. A k-anonymity method, under which only a truncated cryptographic hash prefix is disclosed for comparison, or an equivalent method offering the same guarantee, shall be used.

"53C. Password standard. — (a) A Regulated Entity shall require passwords used as a single-factor authentication mechanism to have a minimum length of fifteen characters, and shall require passwords used only as part of a multi-factor authentication process to have a minimum length of eight characters. (b) A Regulated Entity shall not require a password to contain a specific combination of character types. It may reject passwords consisting solely of sequential or repeated characters. (c) A Regulated Entity shall permit passwords of at least sixty-four characters, and shall permit spaces and the full range of printable ASCII characters. (d) A Regulated Entity shall screen a proposed password against a blocklist of known commonly used, expected or compromised passwords, in the manner described in paragraph 53B(d), and shall reject a password so identified. Such a blocklist need not be exhaustive; it should be sufficient to exclude passwords likely to be guessed before rate-limiting takes effect. (e) A Regulated Entity may offer or require an additional authentication factor at login. Where a second factor is required, the password forms part of a multi-factor authentication process and the eight-character minimum in sub-paragraph (a) applies to it."

(f) A Regulated Entity shall not rely on knowledge-based security questions, including a mother's maiden name, place of birth or first school attended, as an authentication factor or as a sole means of account recovery.

(g) A Regulated Entity shall apply the same password standard to a login password and to any separate transaction password maintained for the same customer relationship.

Drafting note on sub-paragraph (a). NIST SP 800-63B-4 requires a fifteen-character minimum where a password is used as a single-factor authentication mechanism, and requires a minimum of eight characters where the password is used only as part of a multi-factor process. Paragraph 53C follows that distinction and does not impose a higher minimum.

"53D. Password change and statement content. — (a) A Regulated Entity shall provide a self-service facility for a customer to change a login password at any time, without requiring a branch visit. (b) A password change shall take effect immediately and shall trigger a notification to the customer's registered contact channels. (c) A Regulated Entity shall not require re-entry of the existing password more than once during an authenticated password change.

(d) A Regulated Entity shall not print or transmit, on a customer account statement, welcome kit or similar document, a password or PIN derived by a formula that can be reconstructed from other information on, or associated with, that document.

(e) Sub-paragraph (d) does not prevent the use of a Regulated Entity-generated password delivered under paragraph 53, provided it is not formula-derived and the customer is required to change it on first login as that paragraph requires.

(f) A credential set under a policy in force before commencement shall be migrated to conformity at the customer's next authentication event. It need not be proactively reset. Where such a credential has not been used for twelve continuous months, the Regulated Entity may invalidate it after not less than thirty days' notice to the customer."

"53E. Application accessibility and password managers. — (a) Where a Regulated Entity requires a proprietary application for retail login in preference to a general-purpose web browser, that application shall meet a recognised national or international digital accessibility standard. (b) The application shall allow the use of established third-party password managers and autofill functionality, and shall permit the use of the paste function when entering a

password. (c) The Regulated Entity shall provide a non-application, non-branch alternative channel, including at minimum telephone banking with equivalent safeguards, for customers unable to install or operate the application. (d) Where a virtual keyboard is made available under paragraph 51, it shall be offered as an option and shall not be the only means of entering a User ID or password. (e) Where such an application requires its own PIN or passcode separate from the login password, that credential shall receive the same relief under paragraph 53A, on the same basis, and shall not be subject to mandatory rotation once that relief applies."

Drafting note. Sub-paragraph (b) gives effect, for customer-facing applications, to the requirement of NIST SP 800-63B-4, Section 3.1.1.2, that verifiers "SHALL allow the use of password managers and autofill functionality." Sub-paragraph (d) does not disturb paragraph 51, which requires that a virtual keyboard option "should be made available"; it clarifies that the option is additional to, and not a replacement for, ordinary keyboard entry.

"53F. Anti-enumeration and graduated lockout. — (a) In applying paragraph 35, a Regulated Entity shall apply rate-limiting and progressive delay to consecutive failed login attempts, and shall not block access to the account before not fewer than ten consecutive failed attempts have occurred. The delay imposed after a failed attempt shall increase as the account approaches the maximum permitted number of consecutive failed attempts. On successful authentication, the count of previous failed attempts shall be reset. (b) A Regulated Entity shall not disclose, through an error message or otherwise, whether a submitted login identifier corresponds to an existing customer account. (c) Where the login identifier is a Permanent Account Number or another identifier the customer cannot readily change, rate-limiting shall be applied so that response timing or content does not reveal whether the identifier is valid.

(d) Where a Regulated Entity and a group entity regulated by the Securities and Exchange Board of India serve a shared or overlapping customer base, the Regulated Entity shall use reasonable endeavours to align its password policy with that group entity, so that customers meet a consistent policy. (e) Where a Regulated Entity deploys an additional authentication challenge under paragraph 51, that challenge shall be a bot detection and mitigation mechanism effective against automated scripts, and shall not consist of an arithmetic sum or comparable puzzle that an automated script can solve. A Regulated Entity may satisfy paragraph 51 by applying such a challenge, or a step-up authentication factor, selectively in

response to risk signals — including an unrecognised device, an unusual location, or a burst of failed attempts — rather than to every customer at every login.

(f) A Regulated Entity using a Permanent Account Number, mobile number or email address as a login identifier shall apply sub-paragraphs (a) to (c) to that identifier specifically, having regard to the fact that such an identifier may not be changeable by the customer and may be known from other sources."

Drafting note. Paragraph 35 of the Master Direction already requires a Regulated Entity to set a maximum number of failed login attempts after which access is blocked, to have a secure re-activation procedure, and to notify the customer of failed attempts. This paragraph supplements it by addressing enumeration and by requiring a graduated response before blocking.

"53G. Customer notification. — (a) A Regulated Entity shall notify a customer through not fewer than two independent registered contact channels of any password change, new device or application authorisation, or unlock of a locked account. **An email address shall qualify as a registered contact channel for the purposes of this paragraph only after the Regulated Entity has verified control of that email address through an appropriate verification mechanism.** (b) Notification shall be sent at the time of the event, and shall not wait for the customer's next login."

"53H. Credential storage and logging. — (a) A Regulated Entity shall store customer passwords salted and hashed using a password hashing scheme designed for that purpose, with a cost factor set as high as is practical without materially degrading performance, and reviewed periodically as computing performance increases. (b) A Regulated Entity shall maintain logs sufficient to reconstruct the circumstances of a password change, a failed-login lockout, or the application of paragraph 53A to a specific customer, for supervisory and grievance-redressal purposes. (c) Such logs shall be made available to the Reserve Bank on request."

"53I. Annual reporting. — (a) A Regulated Entity applying paragraph 53A shall report annually to the Reserve Bank, in the format it may specify.

(b) The report shall include, at minimum: (i) fraud and unauthorised-transaction incidence among customers subject to the relief; (ii) the number of accounts where compromise was detected by the methodology certified under paragraph 53B, and the action taken; and (iii)

the reduction in password-reset and account-lockout volume attributable to the relief, together with the associated operating cost saving."

"53J. Account recovery. — (a) A Regulated Entity shall provide at least one means of account recovery that does not require a branch visit and does not rely on knowledge-based security questions. (b) Recovery shall be effected through verification on the customer's registered contact channels, or through an equivalent identity verification of comparable assurance. (c) A recovery event shall be notified to the customer under paragraph 53G and shall be logged under paragraph 53H."

"53K. Phishing-resistant authentication. — (a) A Regulated Entity shall make available to retail customers, as an option, at least one phishing-resistant authentication method, including a device-bound cryptographic credential (a passkey) or a security key. (b) This paragraph takes effect eighteen months from the date of commencement of this circular. (c) The comparative study under paragraph 17 shall report on the availability and take-up of such methods."

C. Implementation Timeline

12. The following schedule applies. Each requirement is listed with the date by which it takes effect; the schedule is not in paragraph order. The requirements taking effect at T + 3 months remove existing obligations and can be given effect by parameter change; the removal of mandatory periodic password change is not conditional on certification under paragraph 53B.

Requirement	**Applicable entities**	**Timeline**
Password standard (para 53C); statement password (para 53D)	All Regulated Entities	T + 3 months
Self-service password change (para 53D(a)–(c))	All Regulated Entities	T + 3 months
Anti-enumeration and graduated lockout (para 53F)	All Regulated Entities	T + 6 months
Customer notification (para 53G)	All Regulated Entities	T + 6 months
Session management (para 52(b)–(e))	All Regulated Entities	T + 6 months
Application accessibility and password managers (para 53E)	Entities requiring a proprietary application	T + 9 months
Credential storage and logging (para 53H)	All Regulated Entities	T + 9 months
Detection capability (para 53B) — implementation plan	All Regulated Entities	T + 2 months
Detection capability (para 53B) — full implementation	All Regulated Entities	T + 9 months
Annual reporting (para 53I)	Regulated Entities applying para 53A	First report at T + 12 months
Account recovery (para 53J)	All Regulated Entities	T + 6 months
Phishing-resistant option (para 53K)	All Regulated Entities	T + 18 months

Requirement	Applicable entities	Timeline
No mandatory periodic password change (para 53A)	All Regulated Entities	T + 3 months

D. Transitional and General Provisions

13. Commencement. — This circular comes into force on the date of its final issue ("T").

14. Overriding effect. — This circular prevails over any inconsistent internal policy of a Regulated Entity, and over any inconsistent term of its customer terms and conditions or documentation.

15. Amendment of customer terms. — A Regulated Entity shall amend its customer terms and related documentation to reflect this circular within six months of T.

16. Savings. — Nothing in this circular invalidates any authentication or password-change action taken, or any password set, before the applicable date.

17. Comparative study and reference model. — The Reserve Bank will commission a comparative study of fraud outcomes, disaggregated by root cause, across Regulated Entities with differing password-rotation policies, to be completed within twelve months of T. The study shall address, in particular, the proportion of card and internet fraud attributable to compromise of a static credential as against social engineering, malware, SIM-swap and other vectors, that breakdown not being available from currently published data. Where the study finds that Regulated Entities not applying mandatory rotation do not experience higher fraud incidence, the Reserve Bank will document the credential-risk controls those entities rely upon instead, including breach and compromise detection, login monitoring and session management, and will publish that documentation as a reference model. A Regulated Entity may adopt the reference model under paragraph 53B(b).

18. Scope. — This circular does not address, and shall not be construed to address, account closure terms, joint-account mandates, deposit-product terms, or any matter that is not one of customer authentication or password policy.

19. No charge for reset or unlock. — No charge shall be levied on a customer for a password reset or account unlock arising from a detection mechanism implemented under paragraph 53B.

20. Contravention. — Contravention of this circular shall be dealt with under the provisions of law applicable to contravention of the Master Direction.

21. Regional Rural Banks and co-operative banks. — The Master Direction does not apply to Regional Rural Banks, Urban Co-operative Banks or State and Central Co-operative Banks, and this circular does not extend it to them. The Reserve Bank will separately consider extending equivalent requirements and equivalent relief to those institutions through the instruments applicable to them, on the same basis, with timelines extended by six months, and on the footing that the detection capability required may be discharged through a sponsor bank, a federation to which the entity is affiliated, or a shared utility including a facility of the Institute for Development and Research in Banking Technology. The customers of these institutions bear the same burden as other customers and should receive the same relief.

22. Cooperation and provision of data. — Regulated Entities shall provide the Reserve Bank, promptly and in full, with the data required for the study under paragraph 17, including password-reset and account-lockout volumes, login-related fraud data disaggregated by root cause, and outcomes under the entity's current password policy. Regulated Entities are reminded that the amendments made by this circular are expected to reduce their own operating costs and to improve customer experience, and their cooperation in completing the study without delay is expected accordingly.

23. Interpretation. — This circular forms part of, and shall be read with, the Master Direction. Should the Reserve Bank prefer to give effect to paragraphs 53A to 53K through the Cyber Security Framework in Banks, 2016, or through a new chapter of the Master Direction dealing specifically with customer authentication, these requirements may be transposed into that form without change of substance.

Yours faithfully,

[Name]

Chief General Manager, Department of Supervision, Reserve Bank of India

Annexure B — Draft Circular for Consideration of the Securities and Exchange Board of India

Investor-Facing Authentication and Password Policy (CSCRF Amendment)

SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2026-27/[•] — [Draft for public comment]

To — All Recognised Stock Exchanges, Depositories, Registrars to an Issue and Share Transfer Agents, Mutual Funds and Asset Management Companies, Stockbrokers, Portfolio Managers and other SEBI Regulated Entities to which the Cybersecurity and Cyber Resilience Framework applies

Madam / Dear Sir,

Amendment to the Cybersecurity and Cyber Resilience Framework (CSCRF) — Investor-facing authentication and password policy

A. Background

1. Please refer to the Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated 20 August 2024), as amended ("the Framework"), and to its five-tier classification of Regulated Entities.

2. Please also refer to the Cyber Security and Cyber Resilience framework for Stockbrokers (SEBI/HO/MIRSD/CIR/PB/2018/147 dated 3 December 2018), under which two-factor authentication is required on applications offered to customers through Internet Based Trading and Securities Trading through Wireless Technology, on every login session.

3. On a review of investor-facing password policy, it is observed that practice varies materially between Regulated Entities, in a manner not explained by the Framework's existing risk tiering. An investor holding both a banking relationship and an affiliated broking or asset-management relationship frequently meets inconsistent password requirements across what is, for the investor, a single relationship.

4. It is further observed that NIST Special Publication 800-63B-4, published on 31 July 2025, provides at Section 3.1.1.2 that verifiers and credential service providers "SHALL NOT require subscribers to change passwords periodically," and "SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords." The case for giving effect to this position, addressed in a parallel draft under consideration by the Reserve Bank of India, applies equally to investor-facing login.

5. It is also observed that removing mandatory rotation is expected to reduce Regulated Entities' operating costs and to improve investor experience. It is clarified that the PCI Data Security Standard is referred to in the accompanying paper only as evidence of the direction of industry practice; Requirement 8 of that Standard governs personnel and third-party access and does not apply to investor accounts.

6. In exercise of the powers conferred by Section 11(1) read with Sections 11(2)(i) and 11A of the Securities and Exchange Board of India Act, 1992, Section 19 of the Depositories Act, 1996, and Section 10 of the Securities Contracts (Regulation) Act, 1956 to the extent it empowers the Board to direct recognised stock exchanges to amend their bye-laws, the Board hereby amends the Framework as follows.

B. New Standard: Investor-Facing Authentication and Password Policy

7. The following standard is inserted into the Framework, applicable to all Regulated Entities to which the Framework applies, calibrated by reference to the Framework's five-tier classification:

> "6.1 No mandatory periodic password change. — A Regulated Entity shall not require an investor to change a login password on a fixed calendar schedule. A change may be required where the investor has been notified of, or the Regulated Entity has reason to believe there has been, a compromise."
>
> "6.2 Detection capability. — (a) A Regulated Entity shall implement a compromise-detection methodology comprising, at minimum, screening of investor passwords against a blocklist of known commonly used, expected or compromised passwords using a k-anonymity or equivalent non-disclosure method, and monitoring for anomalous login behaviour. (b) The methodology shall not involve the transfer of any investor password or personal data to a third party in reversible or identifiable form. (c) A Regulated Entity may satisfy this clause by adopting a reference model published by the Reserve Bank of India or by the Board. (d) A Regulated Entity shall record its position with the Board within two months of commencement."
>
> "6.2A Proportionality for smaller Regulated Entities. — (a) A Mid-size, Small-size or Self-certification RE may discharge clause 6.2 through participation in a shared Market Security Operations Centre (Market-SOC) facility recognised by the Board. (b) Clause 6.2 does not apply to such an entity until the Board confirms that a Market-SOC facility offering the required

capability is available to it. (c) This clause does not apply to a Regulated Entity that operates no investor-facing digital platform requiring a login password."

"6.3 Password standard. — A Regulated Entity shall require a minimum password length of fifteen characters where the password is used as a single-factor authentication mechanism and a minimum of eight characters where the password is used only as part of a multi-factor authentication process. It shall not require a specific combination of character types. It shall permit passwords of at least sixty-four characters, and shall permit spaces and the full range of printable ASCII characters. It shall allow the use of password managers and autofill functionality, and shall permit the use of the paste function when entering a password."

Drafting note on clause 6.3. NIST SP 800-63B-4 requires a minimum of fifteen characters where a password is the single authentication factor, and a minimum of eight where it forms part of a multi-factor process. Clause 6.3 follows that distinction and does not impose a higher minimum.

"6.4 Password history. — A Regulated Entity shall not maintain a password-history restriction."

"6.5 Formula-derived passwords. — A Regulated Entity shall not print or transmit, on an investor account statement, contract note, welcome kit or similar document, a password or PIN derived by a formula that can be reconstructed from other information on, or associated with, that document."

"6.6 Legacy credentials. — A credential set under a policy in force before commencement shall be migrated to conformity with clauses 6.1 to 6.4 at the investor's next authentication event. Where unused for twelve continuous months, it may be invalidated after not less than thirty days' notice."

"6.7 Anti-enumeration. — A Regulated Entity shall apply rate-limiting and progressive delay to repeated failed login attempts rather than immediate permanent lockout. It shall not disclose through an error message whether a submitted identifier corresponds to an existing investor account. It shall apply these safeguards with particular care where the identifier is a Permanent Account Number or another identifier the investor cannot readily change."

"6.8 Step-up authentication and session management. — (a) A Regulated Entity shall require an additional authentication factor beyond login only for: (i) addition or modification of a bank

account registered for payout; (ii) addition or modification of a nominee; (iii) change of registered mobile number or email address, including verification of the new email address before it is treated as a registered email channel; (iv) transfer or pledge of holdings to a demat account not previously linked to the investor's profile; and (v) enhancement of a transaction or payout limit. For the avoidance of doubt, nothing in this clause or in this standard requires a second authentication factor for the placement, modification or cancellation of a trading order within an authenticated session. The two-factor authentication required at every login session under the Cyber Security and Cyber Resilience Framework for Stockbrokers, and the operating requirements of the recognised stock exchanges and depositories giving effect to it, are unaffected and remain the applicable control for the trading workflow.

(b) The list in sub-clause (a) is exhaustive. A Regulated Entity shall not extend it by internal policy without the Board's prior approval.

(c) Where an additional factor is required, a Regulated Entity shall offer a non-SMS factor as an option. It shall not require SMS one-time password as the sole second factor. This does not displace the existing requirement that, where a one-time password is used, it be sent to the client by both email and SMS. An email address shall not be used for delivery of a one-time password or other authentication-related communication unless the Regulated Entity has verified control of that email address through an appropriate verification mechanism. Where the email address has not been so verified, the Regulated Entity **shall use another verified registered channel available to the investor.**

(d) Session management shall follow paragraph 52 of the parallel Reserve Bank of India draft. Where a Regulated Entity issues a separate credential for algorithmic or API-based trading, that credential shall be independently revocable by the investor and shall expire not later than twelve months from issue absent renewal."

"6.9 Knowledge-based security questions. — A Regulated Entity shall not rely on knowledge-based security questions as an authentication factor or as a sole means of account recovery, for the reasons stated at paragraph 53C(f) of the parallel Reserve Bank of India draft."

"6.10 Reporting. — A Regulated Entity applying clause 6.1 shall report annually to the Board, proportionately to its classification under the Framework, on terms equivalent to paragraph 53I of the parallel Reserve Bank of India draft, including the reduction in password-reset and lockout volume attributable to the relief."

"6.11 Cooperation and provision of data. — Regulated Entities shall provide the Board, promptly and in full, with data required to assess investor-facing authentication practice, including password-reset and lockout volumes and login-related fraud data disaggregated by root cause. Regulated Entities are reminded that the amendments made by this circular are expected to reduce their operating costs and improve investor experience, and their cooperation is expected accordingly."

C. Role of Market Infrastructure Institutions and Intermediaries

8. Recognised Stock Exchanges, Clearing Corporations and Depositories shall (a) amend their bye-laws and operating circulars as necessary to reflect clauses 6.1 to 6.11; (b) monitor compliance by connected intermediaries; (c) report aggregate compliance status to the Board on the schedule in paragraph 10; and (d) where operating or sponsoring a Market-SOC facility, ensure it can support certification under clause 6.2 for entities relying on clause 6.2A within twelve months of commencement.

9. Depositories and Registrars to an Issue / Share Transfer Agents shall apply clauses 6.1 to 6.11 to any investor-facing login they operate directly, including any online facility for updating nominee or bank-account details.

D. Implementation Timeline

10. This circular shall be implemented according to the timeline in the accompanying schedule. The removal of mandatory periodic password change is not conditional on compliance with clause 6.2.

Requirement	Applicable entities	Timeline
Password standard (cl. 6.3), statement passwords (cl. 6.5)	All Regulated Entities	T + 3 months
Anti-enumeration (cl. 6.7); knowledge-based questions (cl. 6.9)	All Regulated Entities	T + 6 months
Step-up list and session management (cl. 6.8)	All Regulated Entities	T + 9 months
Market-SOC availability (cl. 6.2A)	Market Infrastructure Institutions	T + 12 months
Password history (cl. 6.4); legacy credentials (cl. 6.6)	All Regulated Entities	T + 3 months
Reporting (cl. 6.10); cooperation and data (cl. 6.11)	All Regulated Entities	First report at T + 12 months
No mandatory periodic password change (cl. 6.1)	All Regulated Entities	T + 3 months

E. Transitional and General Provisions

11. Commencement and overriding effect. — This circular comes into force on the date of its final issue ("T"). It prevails over any inconsistent internal policy or investor-facing terms of a Regulated Entity, which shall be amended to conform within six months of T.

12. Savings and scope. — Nothing in this circular invalidates any authentication or password-change action taken, or any password set, before the applicable date. This circular does not address any matter that is not one of investor authentication or password policy.

13. This circular is issued in the interests of investors and of the orderly development and regulation of the securities markets, and forms part of the Cybersecurity and Cyber Resilience Framework.

Yours faithfully,

[Name]

Chief General Manager, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India

Acknowledgements

I sincerely appreciate the encouragement of Dr. Vijay Kelkar, whose support and guidance were instrumental in making this policy paper possible.

I am grateful to Dr. Abhay Pethe for reading this policy paper and providing valuable comments and encouragement.

I also thank Ms. Ratnamala Dam Manna for her insightful critique, which improved this policy paper.

I am also thankful to Shri. Hrishikesh Dhande for arranging the review of this policy paper and coordinating with Ms. Kiran Pardeshi, Mr. Pradeep Nair and the PIC staff for its publication.

About the Author

Umesh Kudalkar is a Pune-based CFA Charterholder and MBA with over 35 years of experience across corporate finance, venture capital, private equity, and public equity investing. He has served as Chief Investment Officer and CEO, advised private equity investment trusts, managed portfolios exceeding USD 500 million, and served on the boards of 23 companies across diverse industries. He is also a CFA Institute volunteer and a member of the Pune International Centre (PIC).

LinkedIn | Mobile: +91 - 9822014992 | **umesh.kudalkar@gmail.com** |

PUNE INTERNATIONAL CENTRE

S.No. 34/A, Behind Centre for Development of Advanced Computing (C-DAC),
Mansarovar, Panchawati, Pashan, Pune, Maharashtra, India 411008