Unified Fintech Forum

POWERING RESPONSIBLE FINTECH

CYBER SECURITY ADVISORY

Safeguarding Payment and Disbursement APIs Against AI-Driven Cyber Fraud

Consolidated guidance for fintechs, NBFCs and payment service providers, drawing on CERT-In advisories, RBI directions and sector experience on cyber-attacks for unauthorised fund transfers.

DATE OF ISSUE	ADDRESSED TO	SEVERITY
November 02, 2026	**All UFF member entities**	**Critical**

ACTION ALERT | SEVERITY: CRITICAL | UFF/ADV/CYBER/2026/002 | October 30, 2026

Unauthorised payouts through compromised payment and disbursement APIs

THE THREAT

It has been observed and reported that attackers have been breaking into fintechs and NBFCs through exposed applications and APIs, stealing the keys these entities use with their bank or payment aggregator, and sending payout instructions from the entity's own whitelisted systems to mule accounts.[1] Agentic AI tools automate the chain, so one operator can hit several entities in a day. Accounts have been drained within minutes of the first transaction. Entities that acted on CERT-In's advisories, blocked the published IOCs and monitored actively have so far avoided losses.

SUGGESTED ACTIONS

Fintechs / Digital Financial Service Providers are advised to take the necessary steps, and to refer to and follow the advisories and instructions issued by regulatory and Government agencies:

(a) **Block all IOCs** published by CERT-In at perimeter firewalls and proxies, in both directions, and re-check blocking each time the lists are updated.

(b) **Enforce multi-factor authentication** (wherever required) on all portals and on administrative and remote access.

(c) **Restrict payout endpoints** to whitelisted source IPs or an approved corporate VPN.

(d) **Find and rotate keys:** search for payment API keys stored in plain text, rotate payment API keys now and move them into an encrypted vault.

(e) **Shrink the attack surface:** take dormant, deprecated and test APIs and administrative interfaces off the internet, and isolate production from UAT.

(f) **Ask your bank or payment aggregator** to enable beneficiary whitelisting on your payout accounts.

(g) **Watch payouts in real time**, especially on weekends and holidays, for amounts just below limits, Re 1 test transfers and bursts to new beneficiaries.

(h) **Report** any past or ongoing incident linked to this campaign, as set out below.

REPORT WITHIN SIX HOURS

(a) **All members:** report cyber incidents to CERT-In within six hours of noticing them or being notified of them.[2]

(b) **NBFCs:** also report cyber incidents to the RBI on the DAKSH platform within six hours of detection.[3]

(c) **Non-bank PSOs, including payment aggregators:** report unusual incidents to the RBI within six hours of detection.[4]

(d) **Other entities:** report to your own regulator as its directions require (for example, SEBI for brokers).

Members are also advised to ask their banks to freeze the receiving accounts at once and to report the fraud on 1930 or cybercrime.gov.in.[5] *Prompt freezes have enabled recovery.*

CONTACTS

CERT-In Incident Response Help Desk	incident@cert-in.org.in | 1800-11-4949 (toll-free) | Fax 1800-11-6969
RBI (NBFCs)	RBI supervisory platform (DAKSH)
Cyber fraud reporting	National Cyber Crime Helpline 1930 | cybercrime.gov.in

This advisory is not legal or technical advice and does not replace members' own regulatory obligations; see the disclaimer in Section 14.

[1] As reported in CERT-In Advisory CIAD-2026-0046, Threat Actors Exploiting Payment and Disbursement APIs for Unauthorized Fund Transfers in BFSI Entities; CERT-In sector advisories with IOCs and detection rules, circulated on 1 and 15 October 2026.

[2] CERT-In Directions No. 20(3)/2022-CERT-In dated 28 April 2022, issued under Section 70B(6) of the Information Technology Act, 2000, para (ii): cyber incidents to be reported within six hours of noticing them or being notified of them.

[3] RBI (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, RBI/DoS/2026-27/461, 31 July 2026.

[4] RBI Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, RBI/DPSS/2024-25/123, 30 July 2024.

[5] National Cyber Crime Reporting Portal (cybercrime.gov.in) and Helpline 1930, operated by the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs. Early reporting allows funds to be put on hold before they leave the mule account.

ANNEXURE: DETAILED GUIDANCE

ADVISORY TO MEMBERS ON CYBER FRAUD AND API SECURITY

Advisory reference	UFF/ADV/CYBER/2026/002
Date of issue	October 30, 2026
Addressed to	All member entities of the Unified Fintech Forum (UFF)
Subject	Safeguards against unauthorised fund transfers through abuse of payment and disbursement APIs, including AI-driven attacks
Severity	**Critical**

INDEX

Section	Title	Page
–	Action Alert	1
–	Abbreviations	2
1	Background and purpose	3
2	Entities at risk and applicability	3
3	How the attack works	3
4	Warning signs at the payment layer	4
5	Application and perimeter security	4
6	Credential and key management	4
7	Access and network controls	4
8	Payment-layer transaction controls	5
9	Monitoring and detection	5
10	Board oversight and third-party risk	6
11	Incident response and reporting	6
12	Priority action plan for members	7
13	References and contact	7
14	Disclaimer	7

Members are advised to circulate this advisory to their Board, senior management, CISO and technology, payments and operations teams. In this advisory, "must" is used only where an RBI or CERT-In requirement is cited, with its reference in a footnote; everything else is guidance that members are advised to adopt as suits their business. Short titles of the instruments cited are expanded in Section 13.

ABBREVIATIONS

The following abbreviations are used in this advisory.

Abbreviation	Full form	Abbreviation	Full form
AI	Artificial Intelligence	**KYC**	Know Your Customer
API	Application Programming Interface	**LSP**	Lending Service Provider
BFSI	Banking, Financial Services and Insurance	**MFA**	Multi-Factor Authentication
C2	Command and Control (attacker servers that direct malicious tools)	**NBFC**	Non-Banking Financial Company
CERT-In	Indian Computer Emergency Response Team	**PA**	Payment Aggregator
CI/CD	Continuous Integration / Continuous Delivery	**PHP**	PHP: Hypertext Preprocessor (a web scripting language)
CIAD	CERT-In Advisory (prefix used in advisory reference numbers)	**PPI**	Prepaid Payment Instrument
CISO	Chief Information Security Officer	**PSO**	Payment System Operator
CSCRF	Cybersecurity and Cyber Resilience Framework (SEBI)	**RBI**	Reserve Bank of India
DAKSH	RBI's supervisory monitoring platform, used for reporting cyber incidents	**Re**	Indian Rupee (singular, as in Re 1)

Abbreviation	Full form	Abbreviation	Full form
DOR	Department of Regulation, RBI (in RBI reference numbers)	**Rs**	Indian Rupees
DoS	Department of Supervision, RBI (in RBI reference numbers)	**SEBI**	Securities and Exchange Board of India
DPSS	Department of Payment and Settlement Systems, RBI (in RBI reference numbers)	**SIEM**	Security Information and Event Management
EDR	Endpoint Detection and Response	**SQL**	Structured Query Language
ICT	Information and Communication Technology	**UAT**	User Acceptance Testing (test environment)
IMPS	Immediate Payment Service	**UFF**	Unified Fintech Forum
IOC	Indicator of Compromise	**VAPT**	Vulnerability Assessment and Penetration Testing
IP	Internet Protocol	**VPN**	Virtual Private Network
IT	Information Technology		

1. BACKGROUND AND PURPOSE

(a) For last few months, cyber criminals have actively been targeting BFSI entities that move money through payment and disbursement APIs. Attackers compromise a fintech or NBFC, steal the credentials it uses with its bank or payment aggregator, and issue genuine-looking payout instructions from the entity's own whitelisted systems to mule accounts.

(b) Experts have advised entities to be vigilant and to follow the necessary steps, particularly non-banks and smaller entities in the financial ecosystem and agencies such as CERT-In have placed its guidance in the public domain, including advisory CIAD-2026-0049 (Critical severity, 15 October 2026)[6] on AI agents as attack vectors and the companion advisory CIAD-2026-0046 on payment and disbursement APIs.[7] Sector advisories with indicators of compromise (IOCs) and detection rules were also circulated on 1 and 15 October 2026.[8]

(c) Experience so far is clear: entities that implemented the advisories, blocked the IOCs and monitored actively saw the attacker reach their systems. Receiving an advisory is not enough; fintechs are advised to implement advisories in letter and spirit.

2. ENTITIES AT RISK AND APPLICABILITY

The campaign has targeted the following. However the list is indicative not exhaustive.

(a) NBFCs and digital lending platforms disbursing loans through APIs.

(b) Payment aggregators, wallet operators and recharge platforms.

(c) Securities brokers offering instant withdrawals and fee-collection platforms.

(d) Business correspondents and any other entity that moves money through bank or payment-aggregator APIs.

(a) **NBFCs and PAs/PSOs** are subject to the RBI requirements cited, as each requirement states. CERT-In requirements (Sections 9 and 11) apply to all categories.

(b) **LSPs:** RBI requirements on digital lending bind the regulated entity on whose behalf the LSP acts. LSPs are advised to apply the same controls to the systems they operate and to support their partner regulated entities in meeting those requirements.

(c) **Brokers/wealth tech** are regulated by SEBI, whose cybersecurity requirements apply in addition and are not covered here. The RBI requirements cited do not apply to them unless they also hold an RBI licence or registration.

(d) **Technology providers** that build, host or operate payment or payout systems for regulated entities are advised to apply these controls and to expect assurance, audit and reporting requests from clients under the clients' outsourcing obligations.

(e) Members that hold more than one licence or role are advised to apply the sections relevant to each.

3. HOW THE ATTACK WORKS

(a) **Reconnaissance:** automated scanning of public websites and public-facing APIs for weaknesses.

(b) **Exploitation:** compromise of internet-facing applications through known flaws such as Oracle WebLogic remote code execution, Apache Struts file upload, SQL injection and PHP vulnerabilities, or through internal and deprecated APIs accidentally left exposed.

[6] CERT-In Advisory CIAD-2026-0049, AI Agents as Attack Vectors, Critical severity, 15 October 2026.
[7] CERT-In Advisory CIAD-2026-0046.
[8] CERT-In sector advisories of 1 and 15 October 2026.

(c) **Persistence and theft:** web shells are planted, and payment API keys are stolen from plaintext configuration files, databases or poorly secured secret stores. Where UAT can reach production, attackers pivot from test to live systems.

(d) **Payout:** payout APIs are invoked from the entity's own whitelisted infrastructure, so the bank or aggregator sees a trusted source. Limits, KYC and beneficiary checks that sit only at the application layer are bypassed.

(e) **Cash-out:** funds move to mule accounts and are withdrawn immediately. Accounts have been drained within 15 to 20 minutes of the first transaction, and within two hours of initial compromise in one case.

(f) **AI automation:** open-source agentic AI frameworks automate the chain from reconnaissance to payout, allowing one operator to hit several entities on the same day. Attacker infrastructure has been traced mainly to foreign jurisdictions, largely behind VPNs.

4. WARNING SIGNS AT THE PAYMENT LAYER

(a) Transfers on weekends and national holidays using 24x7 payment rails.

(b) Amounts capped just below limits, for example Rs 4,99,000 against the Rs 5 lakh IMPS limit[9], or below aggregator caps.

(c) Test transfers of Re 1 (and in some cases Rs 1 lakh) before the main run.

(d) Dummy or reused identifiers where the API requires a reference, and payouts to unfamiliar beneficiaries at high velocity.

(e) Any traffic matching published IOCs. Members are advised to treat such traffic as a suspected compromise and to investigate it fully before closing it as a false positive or a prevented attack.

5. APPLICATION AND PERIMETER SECURITY

Members are advised to take the following measures.

(a) Maintain a complete inventory of all applications and APIs. Audits have missed the very application that was later compromised.

(b) Conduct VAPT of every internet-facing application and API, preferably through a CERT-In empanelled auditor, and close all findings.

(c) Patch internet-facing applications and middleware without delay; fix file-upload and SQL injection weaknesses through input validation.

(d) Decommission dormant, deprecated and test APIs and accounts, and remove management and administrative interfaces from the internet.

(e) **RBI requirement:** NBFCs must carry out vulnerability assessment at least every six months and penetration testing at least every 12 months for critical and customer-facing systems, and also before and after implementation or change, through independent experts, closing findings within set timelines.[10] Non-bank PSOs must follow a secure-by-design development life cycle and security-test applications at least annually and before every deployment.[11]

6. CREDENTIAL AND KEY MANAGEMENT

Members are advised to take the following measures.

(a) Ensure no credential, API key or secret is stored in plain text anywhere, including source code, repository history, CI/CD variables, configuration files and databases.

(b) Move all payment API keys and secrets into a secure, encrypted vault, and rotate them at regular intervals and immediately after any suspected exposure.

(c) Scan every commit and build for secrets; rotate and purge any exposed credential and verify the fix externally.

(d) **RBI requirement:** NBFCs must use strong, internationally accepted and non-deprecated cryptographic algorithms, key lengths and protocols.[12] Non-bank PSOs must change default credentials before go-live, encrypt data at rest and in transit, and rotate privileged credentials.[13]

7. ACCESS AND NETWORK CONTROLS

Members are advised to take the following measures.

(a) Enforce multi-factor authentication on all portals, endpoints and administrative access.

(b) Restrict payout endpoints to whitelisted source IPs or an approved corporate VPN, and block access from outside approved geographies wherever feasible.

(c) Isolate production from UAT and other non-production environments.

[9] The RBI raised the per-transaction limit for IMPS from Rs 2 lakh to Rs 5 lakh in October 2021.
[10] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[11] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).
[12] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[13] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).

(d) Block all published IOCs, including the C2 IP addresses of AI attack tools, at perimeter firewalls and proxies in both directions; restrict non-standard ports and allow egress only to approved destinations; re-verify blocking each time IOC lists are updated.

(e) Put controls in place to prevent intrusion into the network from vendor and partner environments.

(f) **RBI requirement:** The NBFC, based on the risk assessment, shall implement two-factor or multi-factor authentication for privileged users of (i) critical information systems and (ii) for critical activities.[14]

(g) **RBI requirement:** Non-bank Payment System Operators (PSOs) shall ensure that all payment transactions, including cash withdrawals, involving debit to the account conducted through electronic modes (bank accounts / debit cards / credit cards / PPIs, etc.) are permitted only by validation through multi-factor authentication, except where explicitly permitted / relaxed. The use of privileged accounts shall be with multi-factor authentication and tightly monitored. Appropriate controls, including rotation policy, shall be implemented. In case of remote / work from home situations, adequate precautions, including multi-factor authentication mechanism, shall be in place.[15]

8. PAYMENT-LAYER TRANSACTION CONTROLS

These controls are the most effective defence against this campaign. Most need coordination with the member's bank or payment aggregator. Members are advised to put in place the following.

(a) **Beneficiary whitelisting:** register approved beneficiary accounts with the bank or payment aggregator, so that funds cannot be sent to any other account.

(b) **Automated maker-checker:** the bank returns the beneficiary details of each payout through a second API, and the member's system matches them against the genuine customer record before approval. This does not require a human in the loop and need not slow bulk disbursements.

(c) **Reverse validation:** the disbursing bank or aggregator confirms that the loan record or reference number in the payout request actually exists at the application layer.

(d) **Separate channel:** run each such check on a channel independent of the payout server. If both legs pass through the same compromised system, the attacker controls both.

(e) **Regulatory anchor for lenders:** under the NBFC Credit Facilities Directions, 2025 (Chapter III), disbursement of loan by an NBFC shall always be made into the bank account of the borrower except for disbursals covered exclusively under statutory or regulatory mandate (of the Reserve Bank or of any other regulator), flow of money between lenders for co-lending transactions and disbursals for specific end use, provided the loan is disbursed directly into the bank account of the end-beneficiary. An NBFC shall ensure that in no case, disbursal is made to a third-party account, including the accounts of LSP, except as provided for in Chapter III on 'Digital Lending'.[16]

(f) **Payment-system safeguards:** PSOs must validate electronic debits through additional factor authentication unless specifically exempted, show the beneficiary name drawn from the receiving bank's records in transaction alerts, and generate online alerts on transaction velocity, geo-location and IP origin.[17] The NBFC Cybersecurity Directions, 2026 also provide for maker-checker controls on critical activities.[18]

(g) Members are advised to engage their partner banks and payment aggregators on these controls. Major banks and payment aggregators face the same attacks, and some have begun offering such controls.

9. MONITORING AND DETECTION

Members are advised to take the following measures.

(a) Move from end-of-day reconciliation to real-time monitoring and continuous reconciliation of payouts, with alerts that are actively watched.

(b) Apply rate-based and per-second API anomaly detection, and alert on enumeration bursts, bulk reads and automated registrations.

(c) Use AI-assisted EDR and SIEM tools where available, and deploy honeypots for deception where feasible.

(d) **CERT-In requirement:** service providers, intermediaries, data centres, body corporates and government organisations must maintain logs of all their ICT systems securely for a rolling period of 180 days within Indian jurisdiction.[19] **RBI requirement:** non-bank PSOs must retain audit logs for at least five years.[20]

[14] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[15] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).
[16] RBI (Non-Banking Financial Companies – Credit Facilities) Directions, 2025, RBI/DOR/2025-26/347, 28 November 2025 (as updated on 15 July 2026), Chapter III on Digital Lending.
[17] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123); RBI (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, 25 September 2025.
[18] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[19] CERT-In Directions, 2022 (No. 20(3)/2022-CERT-In, 28 April 2022), para (iv): logs of all ICT systems to be maintained securely for a rolling period of 180 days within Indian jurisdiction.
[20] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).

(e) **RBI requirement:** PSOs must run a Security Operations Centre with SIEM-based correlation and a real-time or near real-time fraud monitoring solution.[21] Middle and upper-layer NBFCs must operate an early warning signal framework with real-time or minimal-lag monitoring of non-credit transactions, and close watch on money mule and non-KYC accounts.[22]

10. BOARD OVERSIGHT AND THIRD-PARTY RISK

Members are advised to take the following measures.

(a) Place cyber and payment-fraud risk on the Board agenda.

(b) Assess vendors, cloud providers and other technology partners in proportion to risk, covering concentration risk, single points of failure, customer data protection and supply-chain risk.

(c) Govern any AI agents deployed internally with short-lived, least-privilege identities, default-deny egress and tamper-resistant activity logs, as recommended in CERT-In advisory CIAD-2026-0049.[23]

(d) Conduct periodic crisis communication and incident response drills, and test backups and disaster recovery arrangements.

(e) **RBI requirement:** the Board must approve the cybersecurity strategy, policy and Cyber Crisis Management Plan and review them at least annually, and the CISO, independent of the IT function, must present cyber risk reviews to the Board or its committee every quarter.[24] Outsourcing contracts must provide for monitoring, audit rights and RBI access.[25]

(f) **RBI requirement:** In case of vendors involved in critical processes and activities, the PSO shall obtain certified assurance from an independent auditor on the vendor's cyber resilience capabilities.[26]

11. INCIDENT RESPONSE AND REPORTING

(a) **CERT-In requirement:** service providers, intermediaries, data centres, body corporates and government organisations must report cyber incidents to CERT-In at **incident@cert-in.org.in** within **six hours** of noticing them or being notified of them.[27]

(b) **RBI requirement:** NBFCs must report cyber incidents to the RBI on the DAKSH platform within six hours of detection.[28] Non-bank PSOs must report unusual incidents to the RBI within six hours of detection.[29] Other regulated entities must report as their applicable directions require.

(c) **RBI requirement:** NBFCs must follow NBFC Fraud Risk Management Directions, 2026.[30]

(d) In addition, members are advised to report attempted attacks that were blocked to CERT-In, with the IOCs and techniques observed. This helps CERT-In warn the member of a second wave and enrich alerts for the whole sector.

(e) Members are advised to coordinate immediately with their banks to take necessary action, and to report the fraud on the National Cyber Crime Helpline 1930 or at cybercrime.gov.in,[31] which can trigger holds on funds in transit, followed by a complaint to the police where the fraud is to be pursued. Prompt freezes have enabled recovery of funds.

(f) Members are advised to preserve logs, disk images and other forensic evidence, and not to format or rebuild compromised systems before evidence is secured.

(g) Members are advised to report without further delay any past incident linked to this campaign that has not yet been reported to CERT-In and, where applicable, to the RBI. Members may also share anonymised details of incidents and IOCs with UFF voluntarily; this does not replace any of the reporting above.

[21] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).
[22] RBI (Non-Banking Financial Companies – Fraud Risk Management) Directions, 2026, RBI/DoS/2026-27/463, 31 July 2026.
[23] CERT-In Advisory CIAD-2026-0049.
[24] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[25] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461); RBI Managing Risks in Outsourcing Directions, 2025.
[26] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).
[27] CERT-In Directions, 2022 (No. 20(3)/2022-CERT-In, 28 April 2022), para (ii): cyber incidents to be reported within six hours of noticing them or being notified of them.
[28] NBFC Cybersecurity Directions, 2026 (RBI/DoS/2026-27/461).
[29] PSO Master Directions, 2024 (RBI/DPSS/2024-25/123).
[30] NBFC Fraud Risk Management Directions, 2026 (RBI/DoS/2026-27/463), including the thresholds and manner for reporting frauds to the RBI and to law enforcement agencies.
[31] National Cyber Crime Reporting Portal (cybercrime.gov.in) and Helpline 1930, operated by the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs. Early reporting allows funds to be put on hold before they leave the mule account.

12. PRIORITY ACTION PLAN FOR MEMBERS

Members are advised to track the following internally as a minimum, under the oversight of their own Board.

Priority	Actions
Immediate	Block all published IOCs; enforce MFA; restrict payout endpoints to whitelisted IPs; check for plaintext keys and rotate payment API keys; report any past or ongoing incident.
Near term	Complete application and API inventory; VAPT and patch all internet-facing systems; decommission unused APIs; move keys to a vault; isolate production; begin beneficiary whitelisting and maker-checker discussions with banks and aggregators.
Ongoing	Real-time monitoring and reconciliation; 180-day log retention; periodic key rotation and retesting; third-party and AI-agent governance; review of new IOCs and advisories as issued.

13. REFERENCES AND CONTACT

Short titles used in this advisory are shown in bold.

(a) **CIAD-2026-0049:** CERT-In Advisory CIAD-2026-0049, AI Agents as Attack Vectors, Critical severity, 15 October 2026.

(b) **CIAD-2026-0046:** CERT-In Advisory CIAD-2026-0046, Threat Actors Exploiting Payment and Disbursement APIs for Unauthorized Fund Transfers in BFSI Entities.

(c) **CERT-In sector advisories:** IOCs and detection rules circulated on 1 October and 15 October 2026.

(d) **CERT-In Directions, 2022:** CERT-In Directions No. 20(3)/2022-CERT-In dated 28 April 2022 under Section 70B(6) of the Information Technology Act, 2000, on information security practices and reporting of cyber incidents within six hours.

(e) **NBFC Cybersecurity Directions, 2026:** RBI (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, RBI/DoS/2026-27/461, 31 July 2026, including reporting of cyber incidents on DAKSH within six hours.

(f) **NBFC Fraud Risk Management Directions, 2026:** RBI (Non-Banking Financial Companies – Fraud Risk Management) Directions, 2026, RBI/DoS/2026-27/463, 31 July 2026.

(g) **PSO Master Directions, 2024:** RBI Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, RBI/DPSS/2024-25/123, 30 July 2024, applicable to payment aggregators and other non-bank PSOs.

(h) **Authentication Directions, 2025:** RBI (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, 25 September 2025.

(i) **NBFC Credit Facilities Directions, 2025:** RBI (Non-Banking Financial Companies – Credit Facilities) Directions, 2025, RBI/DOR/2025-26/347, 28 November 2025, as updated on 15 July 2026, Chapter III on digital lending.

(j) **Managing Risks in Outsourcing Directions, 2025:** RBI Managing Risks in Outsourcing Directions, 2025, as applicable to the regulated entity.

(k) **SEBI CSCRF:** SEBI Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities, 20 August 2024, as amended, applicable to securities brokers and other SEBI-regulated entities.

(l) Contacts: CERT-In incident reporting at incident@cert-in.org.in or 1800-11-4949 (toll-free); cyber fraud reporting on the National Cyber Crime Helpline 1930 or at cybercrime.gov.in.

Queries on this advisory may be addressed to UFF at communication@unifiedfintech.in.

14. DISCLAIMER

This advisory is issued by UFF for the information of fintechs. **It is not legal or technical advice**. It is not exhaustive: it does not cover every threat or control relevant to a member's business.

It does not substitute for, modify or interpret members' own obligations under the directions of the RBI, SEBI, CERT-In or any other authority, which each member remains responsible for meeting in full. Where this advisory summarises a regulatory requirement, the text of the source instrument prevails. Members are advised to obtain their own legal and technical advice before acting on it. UFF, its office-bearers and staff accept no liability for any loss or consequence arising from reliance on this advisory, or from any action taken or not taken on the basis of it.