Codec Networks

Coding Threats. Decoding Solutions.

NBFCS & LENDING

Lend Faster. Stay Secure. Stay Compliant.

Regulatory applicability, IT audits, lending platform security, privacy and SOC for NBFCs and lenders

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

RBI's 2026 NBFC Directions, layer by layer

How Codec Networks helps

Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start

Lending is digital, partner-led and layer-regulated

Growth and risk now travel through the same channels

4 layers

Base, Middle, Upper and Top under scale-based regulation

17

NBFCs in RBI's 2026-27 Upper Layer list

6 hours

To report cyber incidents to RBI (NHB for HFCs)

31 Jul 2026

RBI's new cybersecurity Directions for NBFCs

What this means: every NBFC must now map its layer to the right chapter of RBI's 2026 Directions—and prove that its apps, partners and field channels are secure enough for regulators, bank partners and investors.

Sources: RBI press release on the NBFC Upper Layer list (August 2026); RBI NBFC Directions (31 July 2026).

Who we serve across NBFCs and lending

Housing finance

HFCs regulated by RBI, supervised by NHB

Vehicle finance

Car, two-wheeler and commercial vehicles

Microfinance

NBFC-MFIs and field-led lending

Consumer finance

Personal loans, durables and credit lines

Gold loans

Branch-heavy secured lending

Infrastructure lenders

Government and private infrastructure finance

Digital lenders

Lending apps and LSP platforms

Lending technology

LOS, LMS, cloud and data partners

The threats that cost lenders the most

Six priorities from our 18-threat NBFC assessment

Synthetic identity & document fraud

Forged files, fake buyers and dealer collusion

Fake lending apps

Look-alike apps and sites abusing the lender's brand

Lending app & API exposure

Borrower data leaking through apps and partner APIs

Ransomware

Disbursement and collections stop at month-end

Agent & insider misuse

Field devices, exports and collection scripts

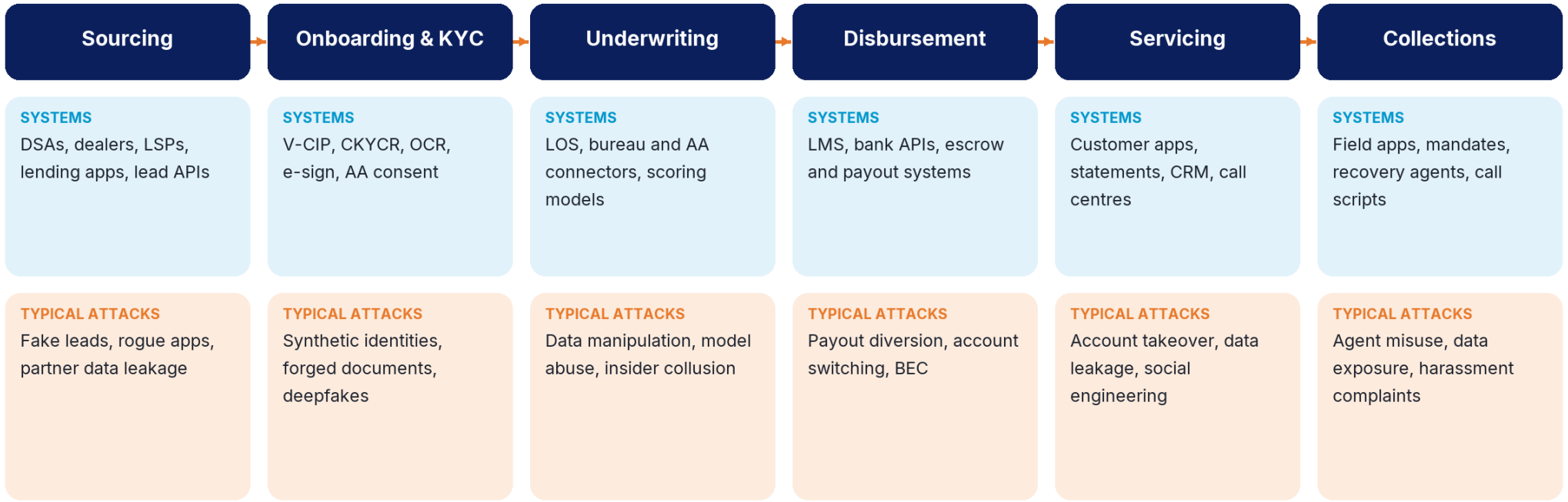
Slow detection & reporting

Missing logs and untested playbooks blow the 6-hour window

Attacks target every stage of the lending lifecycle

Where Cyber Risk Sits in the Lending Lifecycle

Every stage of a loan carries its own attack surface



A lender is only as secure as its weakest partner and its weakest stage—security must follow the loan from lead to closure.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

RBI issued layer-based cybersecurity Directions for NBFCs on 31 July 2026

Codec Networks
Coding Threats. Decoding Solutions.

The 2026 NBFC rulebook, by layer

Requirement	Frequency / deadline	Source
Board-approved technology and cyber policies	Reviewed at least annually	All NBFCs (Chapter II)
Baseline IT controls, BCP and backups	BCP report to Board annually	Base Layer < ₹500 cr and CICs (Chapter III)
IS audit; ITSC meeting	Annually; at least six-monthly	Base Layer ≥ ₹500 cr (Chapter IV)
ITSC of three directors; CISO quarterly review	At least quarterly	Middle Layer and above (Chapter V)
VA / PT of critical systems	Six-monthly / annual	Middle Layer and above
DR drills for critical systems	At least half-yearly	Middle Layer and above
Cyber incident reporting	Within 6 hours (DAKSH; NHB for HFCs)	All NBFCs; CERT-In in parallel
DPDP safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for NBFC Cybersecurity

Key Indian instruments that shape NBFC cybersecurity, audit and assurance

In force Upcoming (from Oct 2026)

Oct 2021	RBI Scale-Based Regulation framework for NBFCs (in force Oct 2022)
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Apr 2024	RBI IT Governance, Risk, Controls and Assurance Master Direction in force
Jul 2024	RBI Master Directions on Fraud Risk Management in NBFCs
May 2025	RBI (Digital Lending) Directions, 2025
Nov 2025	RBI consolidated Master Directions; DPDP Rules notified
Jan 2026	RBI Co-Lending Arrangements Directions, 2025 take effect
Jul 2026	RBI NBFC Cybersecurity, Technology Risk, Resilience & Assurance Directions
Aug 2026	RBI announces 2026-27 NBFC Upper Layer list (17 entities)
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: RBI, NHB, CERT-In, MeitY official notifications. Applicability depends on NBFC layer and type.

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

How Codec Networks helps

Applicability · IT audits · Platform security · Privacy · SOC

Codec Networks
Coding Threats. Decoding Solutions.

One partner across the lending lifecycle

Applicability & IT Audit

Layer-wise RBI 2026 applicability, IS audit, fraud and EWS framework reviews

Lending Platform Security

Lending apps, LOS/LMS and partner API testing; VA/PT

24/7 Managed SOC

SIEM, EDR/XDR, fraud and early-warning signal correlation

Privacy & DPDPA

Borrower data mapping, consent, DLP and breach workflow

Partner Assurance

LSP, DSA, dealer, co-lending and cloud provider reviews

Fraud Forensics

Loan-fraud and collusion investigations, RCA

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **B1** Cyber Assessment & VAPT Assurance
- **B2** Application, API & DevSecOps Security
- **B3** Cloud, Infrastructure & Zero Trust
- **B4** Regulatory Cyber Audit & Compliance
- **B5** GRC, ISO, SOC 2 & PCI DSS Maturity
- **B6** Data Privacy & DPDPA Program
- **B7** Managed SOC, MDR & Threat Monitoring
- **B8** Forensics, Incident Response & Malware RCA
- **B9** Third-Party & Supply-Chain Risk
- **B10** Cyber Simulation, Awareness & Tabletop
- **B11** Emerging Tech, AI & Web3 Security

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Base Layer NBFCs and growing lenders

- Layer applicability assessment (B4)
- Scoped VAPT and retest (B1)
- IT policy and BCP review (B5)
- Risk register and roadmap

Assurance

Middle Layer NBFCs and HFCs

- Six-monthly VA, annual PT (B1)
- Lending app and API testing (B2)
- IS audit evidence pack (B4)
- Extended-hours SOC + IR (B7, B8)

Continuous Resilience

Upper Layer and large NBFCs

- Red teaming and simulations (B1, B10)
- LSP and co-lending assurance (B9)
- 24x7 SOC with fraud correlation (B7)
- Quarterly Board and ITSC reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Middle Layer and above: VA at least six-monthly and PT at least annually for critical and customer-facing systems (RBI 2026 Directions)	Scheduled VA/PT with retest	B1
Base Layer ≥ ₹500 crore: IS audit at least annually; ITSC meeting at least six-monthly	IS audit support and governance review	B4
Cyber incidents to RBI on DAKSH within 6 hours (HFCs to NHB); CERT-In notified	IR retainer, playbooks and reporting support	B7, B8
DR drills for critical systems at least half-yearly; BCP tested at least annually	DR drill observation and recovery testing	B1, B10
Digital lending: DLA and LSP oversight and borrower-data restrictions (Digital Lending Directions 2025)	Lending app, LSP and API assurance	B2, B9
Early warning signals and red-flagging for Middle and Upper Layer NBFCs (Fraud Risk Directions)	EWS review, fraud analytics, forensic audit	B7, B8
DPDP safeguards and breach intimation (from May 2027)	DPDPA programme and breach drills	B6

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Dealer Who Sold Cars That Did Not Exist**	Colluding dealers and agents create fictitious borrowers; analytics and EWS expose the cluster	**B8 · B7 · B4**
2	**The Lending App That Was Not Ours**	A rogue app abuses the lender's brand; monitoring and takedown protect borrowers	**B7 · B10 · B6**
3	**The Collection Agent's Phone**	Field devices leak borrower data; app hardening, MDM and DLP stop it	**B2 · B6 · B7**
4	**The Co-Lending Feed That Was Tampered With**	Altered loan files reach the bank partner; signed exchange and reconciliation catch it	**B9 · B3 · B2**
5	**Ransomware at Month-End**	Disbursement and collections stop; EDR, backups and a rehearsed playbook limit the damage	**B7 · B10 · B8**

Example: breaking a dealer-collusion fraud chain

Case 1: The Dealer Who Sold Cars That Did Not Exist

ILLUSTRATIVE ATTACK PATH

Step 1
A colluding dealer and agents submit loan files for fictitious buyers

→

Step 2
Forged documents and mule bank accounts pass basic checks

→

Step 3
Loans are disbursed directly to the dealer account

→

Step 4
EMIs stop after a few months across a cluster of loans

→

Step 5
Large credit losses; fraud classification and reporting duties

WHERE CONTROLS BREAK THE CHAIN

- Document and identity verification beyond OCR
- Analytics linking dealers, agents, devices and accounts
- Early warning signals and red-flagging under fraud directions
- Forensic audit of the loan cluster and dealer

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: document and identity verification beyond OCR, analytics that link dealers, agents, devices and bank accounts, and whether early warning signals trigger red-flagging and forensic audit in time.

Why NBFCs choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018

Regulation-mapped

Mapped to the layer-specific chapters of RBI's 2026 NBFC Directions, digital lending, fraud, CERT-In and DPDP

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST

How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement

Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

NBFC layer, products, channels, partners and your audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.

Codec Networks
Coding Threats. Decoding Solutions.