Codec Networks

Coding Threats. Decoding Solutions.

CREDIT INFORMATION & FINANCIAL DATA

Protect Every Record. Prove Every Score.

Data access controls, privacy, IT audit, API testing and data integrity and leakage assessments for credit and financial data firms



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CICRA, RBI's 2025–26 Directions, SEBI CSCRF and DPDP

How Codec Networks helps

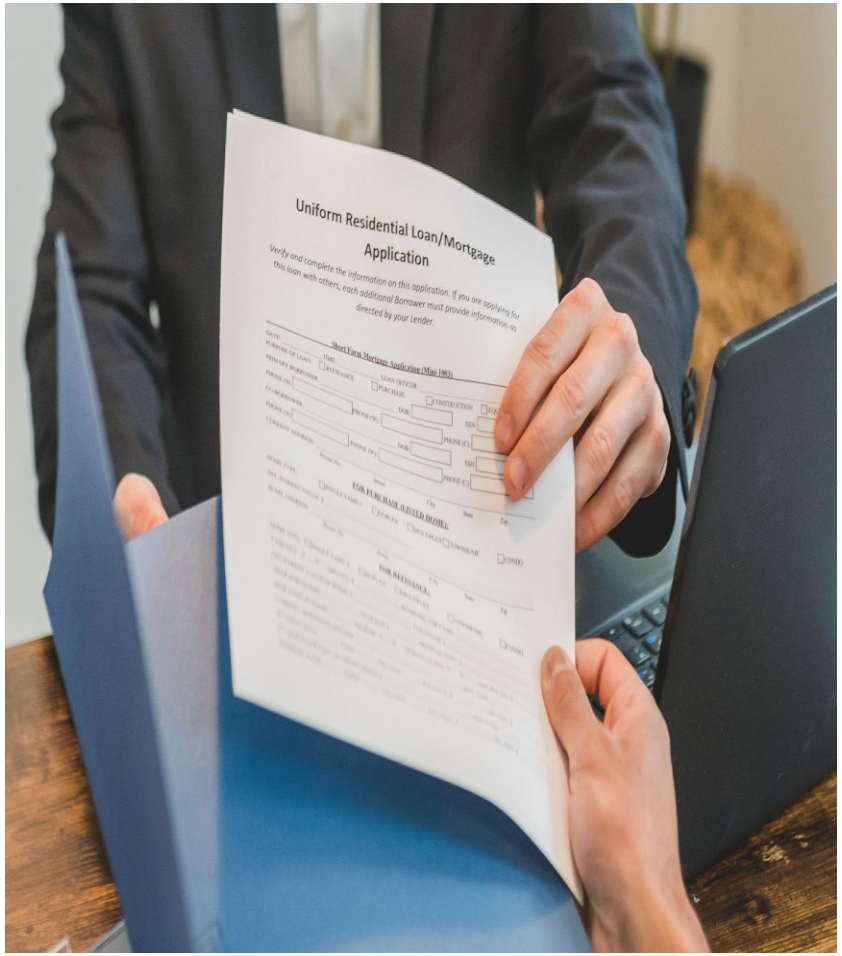
Services, bundles and packages built for the sector

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



Credit data moves faster—and is regulated more closely

Fortnightly reporting, API delivery and new RBI cyber Directions

Fortnightly

Credit data reported by credit institutions to CICs

31 Jul 2026

RBI cyber and technology risk Directions, incl. CICs

6 hours

To report cyber incidents to CERT-In

May 2027

Most DPDP obligations take effect

What this means: credit data firms must control who can access and export data, protect the integrity of every submission, secure report APIs, and be ready to report incidents within six hours—while preparing for DPDP obligations.

Sources: RBI, CERT-In, MeitY; RBI 2026 Direction details as reported in public sources.

Who we serve across credit information and financial data



Credit bureaus

RBI-registered CICs



Credit analytics firms

Scores, models and risk analytics



KYC utilities

Central KYC records



KYC registration agencies

SEBI-regulated KRAs



Financial data processors

Verification and reporting platforms



Reporting lenders

Banks and NBFCs submitting data



Report consumers

Fintechs and lending platforms



Collections partners

Agencies receiving borrower data

The threats that cost credit data firms the most

Six priorities from our 18-threat credit data assessment

Bulk data exfiltration

Millions of records in one breach

API abuse

Unauthorised report pulls at scale

Member credential theft

Trusted keys in the wrong hands

Data tampering

Credit histories rewritten

Insider misuse

Exports for resale

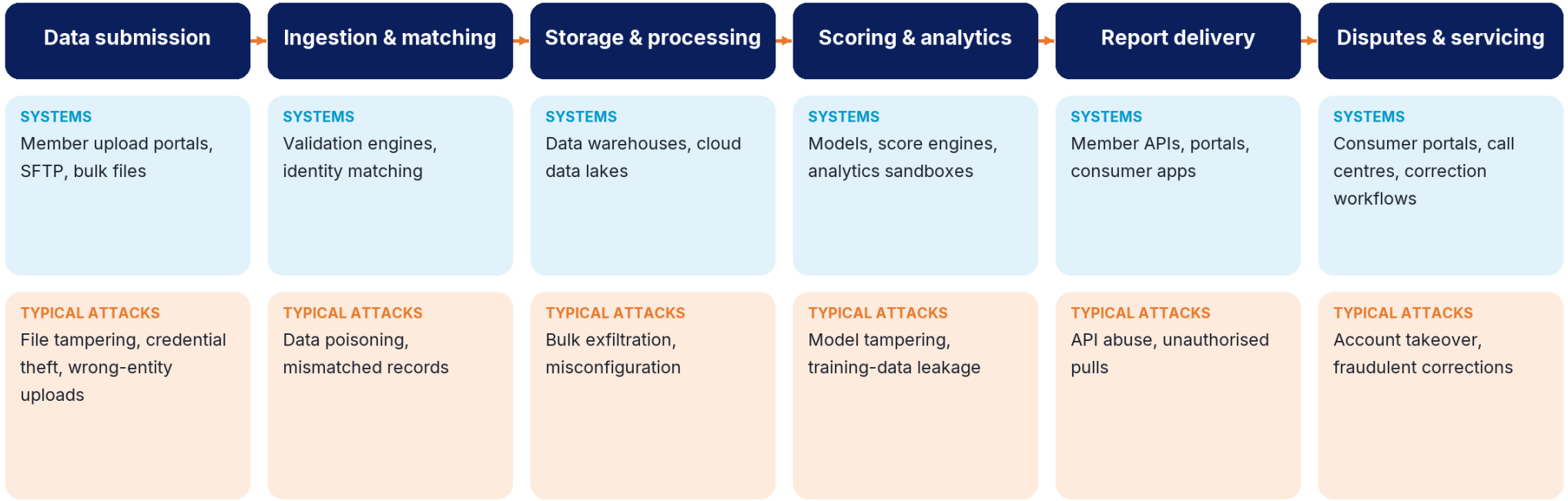
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of the credit data lifecycle

Where Cyber Risk Sits in the Credit Data Lifecycle

Every stage from data submission to decision carries its own attack surface



Credit data is only as trustworthy as the weakest member, API and analyst account that touches it.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CICRA, RBI's 2025–26 Directions, SEBI CSCRF, CERT-In and DPDP

Codec Networks
Coding Threats. Decoding Solutions.

The rules that shape credit data security

Requirement	Frequency / deadline	Source
Security safeguards and privacy principles	Ongoing	CICRA 2005; CIC Regulations 2006
CIC operations and governance	Ongoing	RBI (CIC) Directions, 2025
Credit information reporting	Fortnightly	RBI credit reporting Directions
Cyber, technology risk and assurance	Issued 31 July 2026 (as reported)	RBI framework Directions for CICs
Cyber resilience for KRAs	Per SEBI CSCRF	SEBI CSCRF
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
DPDP safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Codec Networks
Coding Threats. Decoding Solutions.

Key dates on the regulatory timeline

Regulatory Timeline for Credit Information Security

Key RBI, SEBI and cross-sector instruments shaping credit data security

In force Upcoming (from Oct 2026)

2005	Credit Information Companies (Regulation) Act enacted; regulations followed in 2006
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Jan 2025	Credit institutions report credit information to CICs fortnightly
Nov 2025	DPDP Rules, 2025 notified with phased commencement
Jul 2026	RBI cybersecurity, technology risk and assurance Directions, including for CICs (31 July)
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: RBI, SEBI, CERT-In, MeitY. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Data access · Privacy · IT audit · API testing · Integrity · Leakage

Codec Networks
Coding Threats. Decoding Solutions.

One partner across the credit data lifecycle



Data Access Controls

Privileged, analyst and member access reviews



Privacy & DPDPA

Consent, purpose limits, retention, breach workflow



IT Audit

RBI, CICRA and SEBI-aligned IS audits



API Testing

Report, upload and dispute APIs



Data Integrity

Submission files, pipelines, model change



Leakage Assessments

DLP, test data, cloud and data lakes

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

Analytics firms and data processors

- Access and leakage assessment (B6)
- API and app testing (B2)
- ISO 27001 pack (B5)
- DPDPA quick assessment (B6)

Assurance

KYC utilities, KRAs and mid-sized processors

- IS audit and closure (B4)
- API and integrity testing (B2)
- Cloud and data-lake review (B3)
- 24x7 managed SOC (B7)

Continuous Resilience

Credit bureaus and large data platforms

- Red teaming and simulations (B1, B10)
- Member and vendor assurance (B9)
- SOC with insider signals (B7)
- Board and regulator reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Security safeguards and privacy principles for credit information (CICRA 2005, CIC Regulations 2006)	IT audit and data access control review	B4
RBI cyber, technology risk and assurance framework for CICs (July 2026, as reported)	Gap assessment and audit support	B4, B5
Secure report delivery to members and consumers	API and application security testing	B2
Cyber incidents to CERT-In within six hours; 180-day logs	SOC monitoring, IR retainer and reporting support	B7, B8
SEBI CSCRF for KYC registration agencies	CSCRF gap assessment and audit support	B4
Third-party and outsourcing controls	Vendor and member assurance programme	B9
DPDP consent, safeguards and breach intimation	DPDPA programme and leakage assessment	B6

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Member Key That Pulled a Million Reports**	A leaked lender API key pulls reports for weeks; secrets control and pull baselines stop it	B2 · B7 · B8
2	**The Analyst Who Exported the Segment**	An insider exports customer segments; least privilege, DLP and UEBA catch it	B6 · B7 · B8
3	**The Repayment File That Rewrote Histories**	A tampered upload clears defaults; integrity checks and reconciliation prevent it	B2 · B4 · B7
4	**The KYC Records in the Test Bucket**	Production KYC data leaks from test storage; masking and posture monitoring prevent it	B3 · B6 · B8
5	**The Score Model Trained on Stolen Data**	A vendor leaks training data; sharing agreements and vendor reviews prevent it	B9 · B6 · B11

Example: breaking a credential-abuse chain

Case 1: The Member Key That Pulled a Million Reports

ILLUSTRATIVE ATTACK PATH

Step 1
A small lender's API credentials are stored in a code repository

→

Step 2
An attacker finds them and starts pulling credit reports

→

Step 3
Pulls stay below per-minute limits and run for weeks

→

Step 4
Report data is used for targeted loan-fraud calls

→

Step 5
Bureau suspends the member and investigates

WHERE CONTROLS BREAK THE CHAIN

- Secrets scanning and vaulting for member credentials
- Per-member behavioural baselines on report pulls
- Consent and purpose checks on every enquiry
- Rapid member credential revocation playbook

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

Codec Networks

What we test: secrets in code and pipelines, member key rotation and revocation, per-member pull baselines, consent and purpose checks on enquiries, and the six-hour CERT-In reporting step.

Why credit data firms 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 CICRA, RBI, SEBI, 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

Entity type, data flows, member integrations, platforms and 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.