Codec Networks

Coding Threats. Decoding Solutions.

PAYMENTS & FINTECH

Secure Every Transaction. Prove Every Control.

Payment security, regulatory audits, and API & cloud assurance for payment aggregators, PSOs, wallets, processors and lending platforms

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

RBI, CERT-In and DPDP obligations and their timelines

How Codec Networks helps

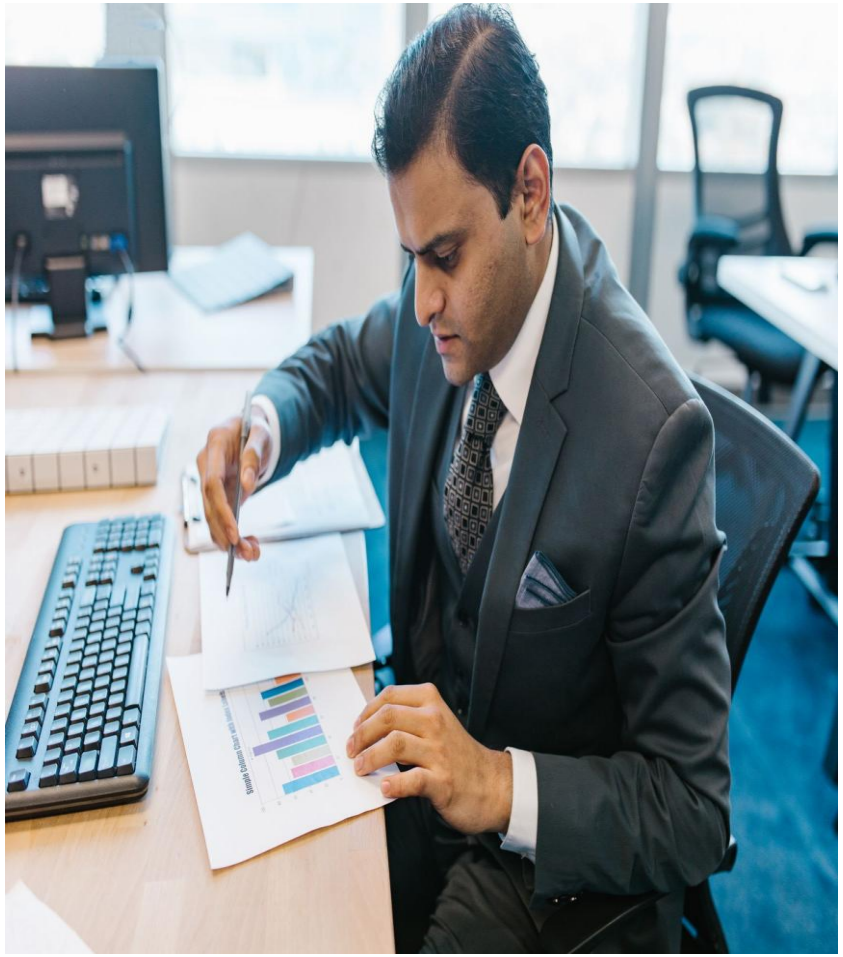
Services, bundles and packages built for the sector

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



A real-time payment economy, at national scale

Speed is the industry's strength—and its biggest security challenge

24.51 bn

UPI transactions in August 2026 (NPCI data)

₹29.82 lakh cr

UPI value processed in August 2026

500 mn+

Account Aggregator consents fulfilled (Sahamati, Sept 2026)

₹19,813 cr

Reported cyber-fraud losses in 2025 (I4C data)

What this means: a single weakness anywhere in the chain—app, aggregator, gateway, network, wallet or lender—can be exploited at the same speed money moves. Regulators now expect detection, reporting and response within hours.

Sources: NPCI monthly statistics; Sahamati press release (Sept 2026); reports based on I4C data (2026). Figures cover all channels where stated.

Who we serve across payments and transaction processing

Payment aggregators

PA-O, PA-P, PA-CB and payment gateways

Payment system operators

Networks, switches, BBPOUs, ATM networks, TReDS

PPI issuers & wallets

Wallets, prepaid and transit cards

UPI apps & processors

TPAPs, card and UPI processors, tokenisation

Digital lending platforms

Lenders, LSPs, DLAs, multi-lender marketplaces

Account Aggregators

Consent platforms and FIP/FIU data flows

Cross-border players

PA-CB, MTSS and remittance platforms

Fintech infrastructure

KYC, V-CIP, BaaS, API and SaaS providers

The threats that cost payment companies the most

Six priorities from our 18-threat sector assessment

Account takeover

SIM swap, OTP theft and remote-access apps defeat weak device binding

Mule merchants & accounts

Borrowed or synthetic identities used to collect and move scam proceeds

API abuse

Broken object-level authorisation exposes every customer through one flaw

E-skimming & SDKs

Altered third-party scripts copy card data at checkout

Cloud misconfiguration

Public buckets, over-privileged roles and leaked secrets

Slow detection & response

Missing logs and untested playbooks blow the 6-hour reporting window

Attacks target every stage of the payment lifecycle

Where Cyber Risk Sits in a Digital Payment

Every stage of the transaction lifecycle has its own attack surface

Onboarding	Initiation	Authentication	Authorisation	Clearing & settlement	Reconciliation & disputes
SYSTEMS Customer & merchant KYC, V-CIP, device binding	**SYSTEMS** App, checkout page, QR, SDK, API call	**SYSTEMS** PIN, OTP, biometrics, device factors	**SYSTEMS** Issuer / PPI / lender decisioning, risk engine	**SYSTEMS** Switches, escrow, nodal & settlement files	**SYSTEMS** Refunds, chargebacks, grievance handling
TYPICAL ATTACKS Synthetic identities, mule merchants, deepfake V-CIP	**TYPICAL ATTACKS** Malicious SDKs, e-skimming, fake QR / collect requests	**TYPICAL ATTACKS** SIM swap, OTP theft, social engineering, remote-access apps	**TYPICAL ATTACKS** Business-logic abuse, limit bypass, API tampering	**TYPICAL ATTACKS** Settlement-file tampering, privileged misuse, insider fraud	**TYPICAL ATTACKS** Refund abuse, account takeover, delayed detection

Security controls must follow the money end to end: a strong authentication step cannot compensate for a weak onboarding, API or settlement control.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

Cybersecurity is a condition of authorisation, partnership and growth

Codec Networks
Coding Threats. Decoding Solutions.

The rulebook has changed—and it keeps a calendar

Requirement	Frequency / deadline	Source
System audit incl. cyber security audit by CERT-In empanelled auditors	Annual	RBI PA Master Direction (15 Sep 2025)
VAPT reports	Half-yearly	RBI PA Master Direction (15 Sep 2025)
Security testing (code review, VA, PT) in authenticated mode	At least annually and before new critical services	RBI cyber resilience directions, non-bank PSOs (30 Jul 2024)
Incident reporting to RBI and CERT-In	Within 6 hours	RBI 2024 directions; CERT-In Directions (Apr 2022)
Backup restoration tests and DR drills	At least half-yearly	RBI 2024 directions
Two-factor authentication with a dynamic factor	In force from 1 Apr 2026	RBI Authentication Directions (Sep 2025)
ICT logs in India / audit log retention	180 days / at least 5 years	CERT-In Directions / RBI 2024 directions
DPDP security safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Payments & Transaction Processing Cybersecurity

Key Indian instruments that create security, audit and assurance obligations

In force Upcoming (from Oct 2026)

Apr 2018	RBI: Storage of Payment System Data (data localisation, SAR by CERT-In empanelled auditor)
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day logs in India, clock sync
Oct 2022	Card-on-File Tokenisation takes effect for online card payments
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Jul 2024	RBI Master Directions on Cyber Resilience & Digital Payment Security Controls for non-bank PSOs
Aug 2024	RBI recognises FACE as the first Self-Regulatory Organisation for FinTech (SRO-FT)
Apr 2025	Large non-bank PSOs (incl. PAs, large PPI issuers, card networks) to comply with the 2024 Directions
May 2025	RBI (Digital Lending) Directions, 2025 consolidate the digital lending framework
Sep 2025	RBI Master Direction on Payment Aggregators (PA-P, PA-O, PA-CB) and Authentication Directions issued
Nov 2025	DPDP Rules, 2025 notified with phased commencement
Apr 2026	Authentication Directions in force; medium non-bank PSOs to comply with the 2024 Directions
Jan 2027	**Revised RBI customer-protection framework for fraudulent electronic banking transactions (banks)**
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect (18 months after notification)**
Apr 2028	**Small non-bank PSOs to comply with the 2024 Directions**

Sources: RBI, CERT-In, MeitY official notifications. Applicability depends on entity type and regulated activity.

Codec Networks

How Codec Networks helps

Payment security · Regulatory audits · API & cloud assurance

Codec Networks
Coding Threats. Decoding Solutions.

One partner for the whole payment chain

Payment & App Security

Web, mobile and API testing; checkout and payment-page security; UPI and wallet app testing

Regulatory Cyber Audits

Cyber and system audits as a CERT-In empanelled auditor; payment data storage audits; PCI DSS

API & Cloud Assurance

Cloud posture, Kubernetes and serverless testing; IAM, secrets and key management

24/7 Managed SOC

SIEM, EDR/XDR, SOAR; fraud-signal correlation; brand and rogue-app monitoring

Forensics & Response

Incident triage, evidence preservation, mule-merchant investigations, RCA

Privacy & Governance

DPDPA readiness, vendor risk, ISO 27001, SOC 2, Board reporting

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

Startups, technology providers, applicants for authorisation

- Scoped VAPT and retest (B1)
- ISO 27001 / PCI DSS gap review (B5)
- Single-account cloud review (B3)
- Assessment report and roadmap

Assurance

Authorised mid-sized PAs, PPI issuers and lenders

- Half-yearly VAPT, app and API testing (B1, B2)
- Annual regulatory cyber audit (B4)
- Cloud posture and DPDPA readiness (B3, B6)
- Extended-hours SOC + IR retainer (B7, B8)

Continuous Resilience

Large PSOs, networks, processors, multi-licence fintechs

- Continuous testing and red teaming (B1, B2, B10)
- Multi-licence audit calendar, vendor assurance (B4, B9)
- 24x7 SOC with fraud-signal correlation (B7)
- Quarterly Board sub-committee reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Annual system and cyber audit by CERT-In empanelled auditors	Regulatory cyber audit with closure tracking	B4
Half-yearly VAPT reports	Scheduled VAPT with retest	B1
Annual authenticated testing; pre-go-live testing	Authenticated VAPT and secure code review	B1, B2
SOC, real-time fraud monitoring, 6-hour reporting	Managed SOC and incident response retainer	B7, B8
Critical-vendor assurance; annual cloud provider audits	Third-party and cloud assurance	B9, B3
PCI DSS / PCI SSF where applicable; payment data in India	PCI DSS readiness; payment data storage audit	B5, B4
DPDP safeguards and breach intimation	DPDPA programme and breach drills	B6

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Merchant That Was Never a Merchant**	Mule merchants pass simplified onboarding; profile-based monitoring and graduated settlement break the chain	**B4 · B7 · B8**
2	**Skimmed at Checkout, Compliant on Paper**	An altered third-party script steals card data; PCI DSS 6.4.3 and 11.6.1 controls catch it	**B5 · B2 · B7**
3	**One API Call Away from Every Borrower's File**	Broken object-level authorisation exposes borrower documents; per-release API testing prevents it	**B2 · B6 · B8**
4	**The Wallet Takeover That Beat the OTP**	SIM swap plus a remote-access app; device binding, cooling periods and dynamic factors stop it	**B2 · B10 · B7**
5	**Six Hours on the Clock**	A public log bucket leaks keys; posture monitoring and a rehearsed 6-hour playbook contain it	**B3 · B7 · B8**

Example: breaking a wallet takeover chain

Case 4: The Wallet Takeover That Beat the OTP

ILLUSTRATIVE ATTACK PATH

Step 1
Customer's SIM is swapped or a screen-sharing app is installed under a pretext

→

Step 2
Attacker receives OTPs and changes the registered mobile number

→

Step 3
New device is bound to the wallet; KYC upgraded with stolen documents

→

Step 4
Balance and linked credit are drained through P2P and merchant transfers

→

Step 5
Customer disputes; issuer bears losses and reputational damage

WHERE CONTROLS BREAK THE CHAIN

- Device binding and SIM-change signals in risk scoring
- 12-hour cooling period after mobile or e-mail change (RBI 2024 Directions)
- Blocking transactions while remote-access apps are active
- Dynamic, risk-based second factor under the 2025 Authentication Directions

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

Codec Networks

What we test: device binding, the 12-hour cooling period after a mobile number or e-mail change, remote-access app detection and the dynamic second factor required from 1 April 2026.

Why payments and transaction processing teams 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

Every finding mapped to RBI, NPCI, CERT-In, DPDP and PCI DSS obligations

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

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

Fintech-grade 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 sub-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 partner banks
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Licences, products, money flows, critical systems 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 authorisation and category.

Codec Networks
Coding Threats. Decoding Solutions.