

Codec Networks

Coding Threats. Decoding Solutions.

FINTECH & DIGITAL FINANCIAL SERVICES

Build Fast. Ship Secure. Pass Every Diligence.

API security, cloud assessment, DevSecOps, TPRM, fraud simulations and regulatory readiness for fintechs

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

Digital lending rules, partners' RBI obligations, CERT-In and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



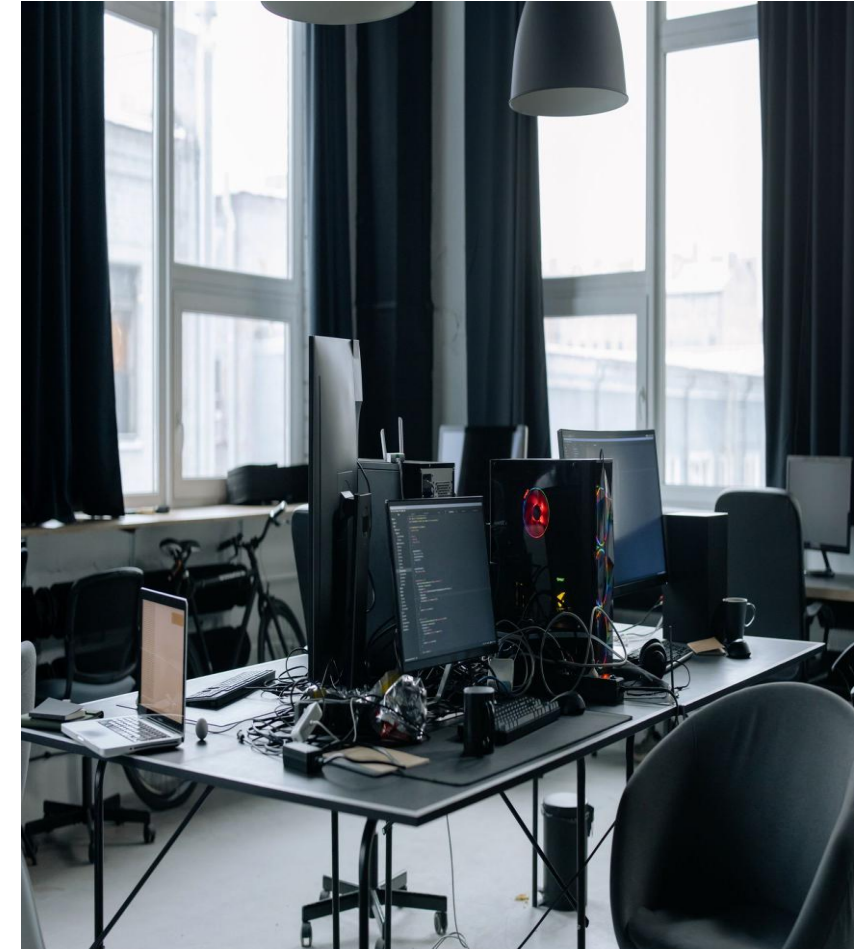
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Fintech is API-first, partner-led and data-rich

Speed and integration are the strengths—and the attack surface

500 mn+

Account Aggregator consents
fulfilled (Sahamati, Sept 2026)

1,100+

Regulated entities live on the AA
ecosystem

6 hours

To report specified incidents to
CERT-In

May 2027

Most DPDP Rules obligations
take effect

What this means: fintechs must prove security to every regulated partner, investor and enterprise customer—while shipping weekly and handling consented financial data under India's new privacy rules.

Sources: Sahamati press release (September 2026); CERT-In Directions (2022); DPDP Rules (2025).

Who we serve across fintech



Lending technology

LSPs and lending platforms



Account Aggregators

Consent and data-flow platforms



Embedded finance

Credit and payments inside apps



Financial APIs & BaaS

KYC, data and banking APIs



P2P lending

RBI-registered marketplaces



KYC & identity

e-KYC, V-CIP and verification



Wealthtech & insurtech

Investment and insurance apps



Fintech SaaS

Platforms sold to banks and NBFCs

The threats that cost fintechs the most

Six priorities from our 18-threat fintech assessment



API authorisation flaws

One broken check exposes every customer's data



Leaked keys & secrets

Credentials in repos, logs and apps



Cloud misconfiguration

Public buckets and over-privileged roles



Malicious SDKs

Supply-chain code inside your app



Deepfake & synthetic KYC

AI-generated identities defeat onboarding



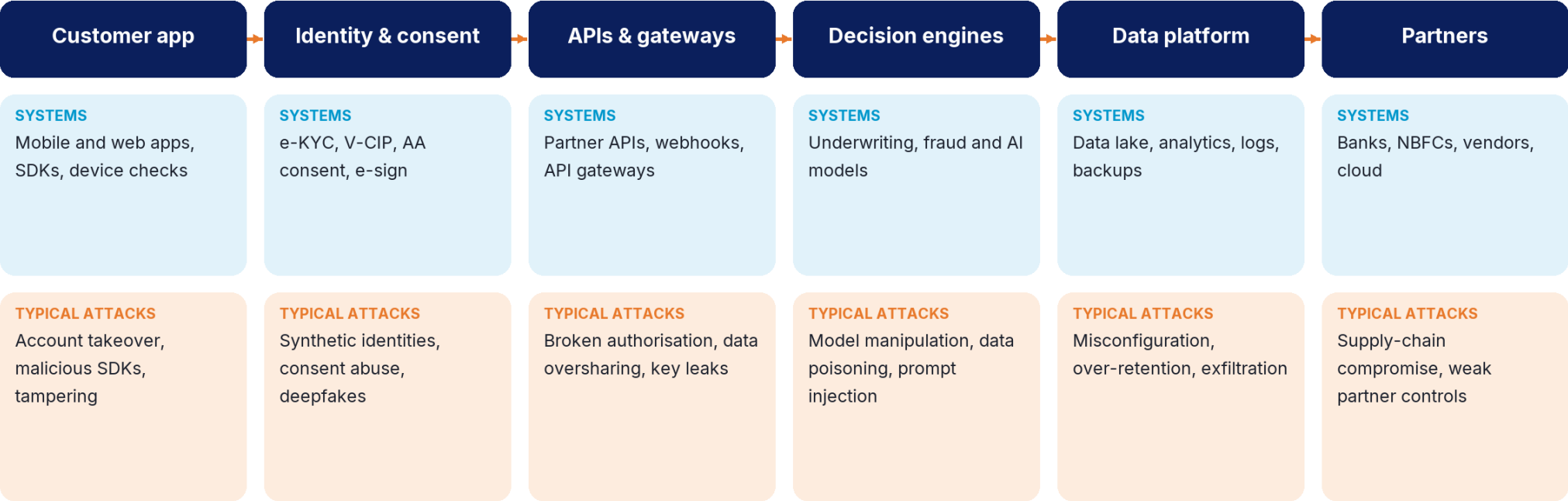
Consent & data misuse

Over-collection and over-retention under DPDP

Attacks target every layer of a fintech platform

Where Cyber Risk Sits in a Fintech Platform

Each layer of a fintech product carries its own attack surface



A fintech's risk travels through its APIs and partners—security must cover the product, the platform and every integration.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Fintech security is judged by partners, regulators and India's new privacy law

The rules that shape fintech security

Requirement	Frequency / deadline	Source
Lender accountability for LSPs; borrower-data restrictions	In force since 8 May 2025	RBI Digital Lending Directions
DLA reporting on RBI's CIMS portal	From 15 June 2025	RBI Digital Lending Directions
Cyber requirements for NBFC-AAs and NBFC-P2Ps	By layer, from 31 Jul 2026	RBI 2026 NBFC Directions
Incident reporting by licensed NBFCs	Within 6 hours (DAKSH)	RBI 2026 NBFC Directions
Specified incident reporting	Within 6 hours	CERT-In Directions (2022)
ICT log retention in India	Rolling 180 days	CERT-In Directions (2022)
Partner oversight, audit and access rights	Ongoing	Bank and NBFC outsourcing rules
Consent, safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Fintech Cybersecurity

Key Indian instruments shaping fintech security, privacy and assurance



Sources: RBI, CERT-In, MeitY official notifications; Sahamati. Applicability depends on licence and partner arrangements.

Codec Networks

How Codec Networks helps

API security · Cloud · DevSecOps · TPRM · Fraud simulation · Readiness

Security that keeps pace with your releases



API & AppSec

REST, GraphQL, webhooks, mobile apps and SDKs



Cloud Assessment

Posture, Kubernetes, IAM and secrets



DevSecOps

SAST, DAST, SCA and secrets scanning in CI/CD



Third-Party Risk

Vendors, SDKs and partner questionnaires



Fraud Simulations

Synthetic identity, deepfake KYC, ATO



Regulatory Readiness

Digital lending, NBFC-AA/P2P, ISO 27001, SOC 2, DPDPA

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

Seed and early-stage fintechs

- Pre-launch API and app VAPT (B1, B2)
- Cloud quick review (B3)
- ISO 27001 / SOC 2 gap review (B5)
- Partner questionnaire pack

Assurance

Growth-stage fintechs and NBFC-AAs

- Release-based testing (B2)
- DevSecOps and secrets scanning (B2)
- DPDPA and TPRM (B6, B9)
- Extended-hours SOC + IR (B7, B8)

Continuous Resilience

Scale-ups and multi-partner platforms

- Red teaming and simulations (B1, B10)
- Continuous cloud assurance (B3)
- 24x7 SOC with fraud correlation (B7)
- Board and investor reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Digital Lending Directions 2025: lenders accountable for LSPs; borrower-data restrictions	LSP security assessment, data-flow and API review	B2, B6
RBI 2026 NBFC Directions: requirements by layer for NBFC-AAs and NBFC-P2Ps	Applicability assessment and gap remediation	B4
Bank and NBFC partner due diligence, audit rights and security controls	Partner-ready assurance pack, VAPT, ISO 27001 / SOC 2	B1, B5
CERT-In: 6-hour reporting, 180-day ICT logs in India, clock sync	Logging review, IR retainer, playbooks	B7, B8
Cloud and secrets security across the platform	Cloud posture, IAM and secrets reviews	B3
DPDP Act and Rules: consent, minimisation, safeguards, breach intimation	DPDPA programme and breach drills	B6
Vendor and SDK supply-chain risk	TPRM and software composition analysis	B9, B2

Five new case studies, five broken chains

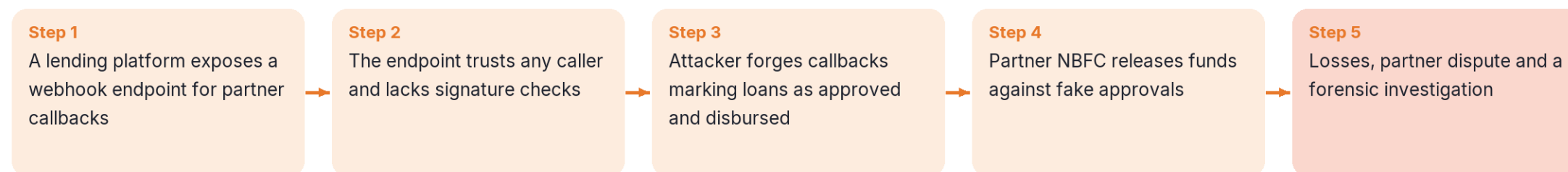
Illustrative composite scenarios written for 2026—not client engagements

1	The Webhook Nobody Owned	Forged partner callbacks mark fake loans as approved; signed webhooks and API ownership stop it	B2 · B7 · B8
2	Consent Given Once, Data Used Forever	Over-retained AA data leaks through a vendor; purpose-bound consent and minimisation prevent it	B6 · B9 · B3
3	The SDK That Phoned Home	A malicious SDK update steals session tokens; SCA and runtime monitoring catch it	B2 · B9 · B7
4	The Deepfake Borrower	Injected video beats liveness; attestation, analytics and deepfake testing close the gap	B10 · B11 · B7
5	The Leaked Key in a Public Repository	A committed cloud key exposes KYC files; secrets scanning and posture monitoring prevent it	B3 · B2 · B8

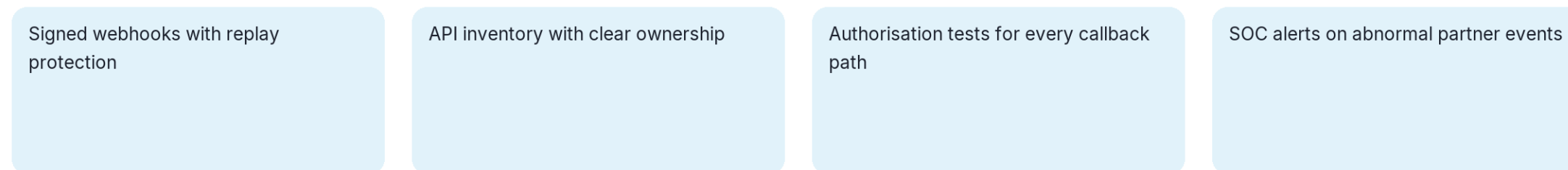
Example: breaking a forged-webhook fraud chain

Case 1: The Webhook Nobody Owned

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: webhook signature and replay protection, authorisation on every partner callback path, API inventory and ownership, and whether the SOC alerts on abnormal partner events before funds move.

Why fintechs choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to digital lending rules, partners' RBI obligations, CERT-In, DPDP, ISO 27001 and SOC 2



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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Product, partners, APIs, cloud stack and your diligence deadlines

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.