

Codec Networks

Coding Threats. Decoding Solutions.

BANKING

Protect Every Channel. Prove Every Control.

Regulatory assurance, VAPT, 24/7 SOC and resilience for commercial, small finance, payments and co-operative banks

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

RBI's 2026 cybersecurity Directions and related obligations



How Codec Networks helps

Services, bundles and packages built for the sector



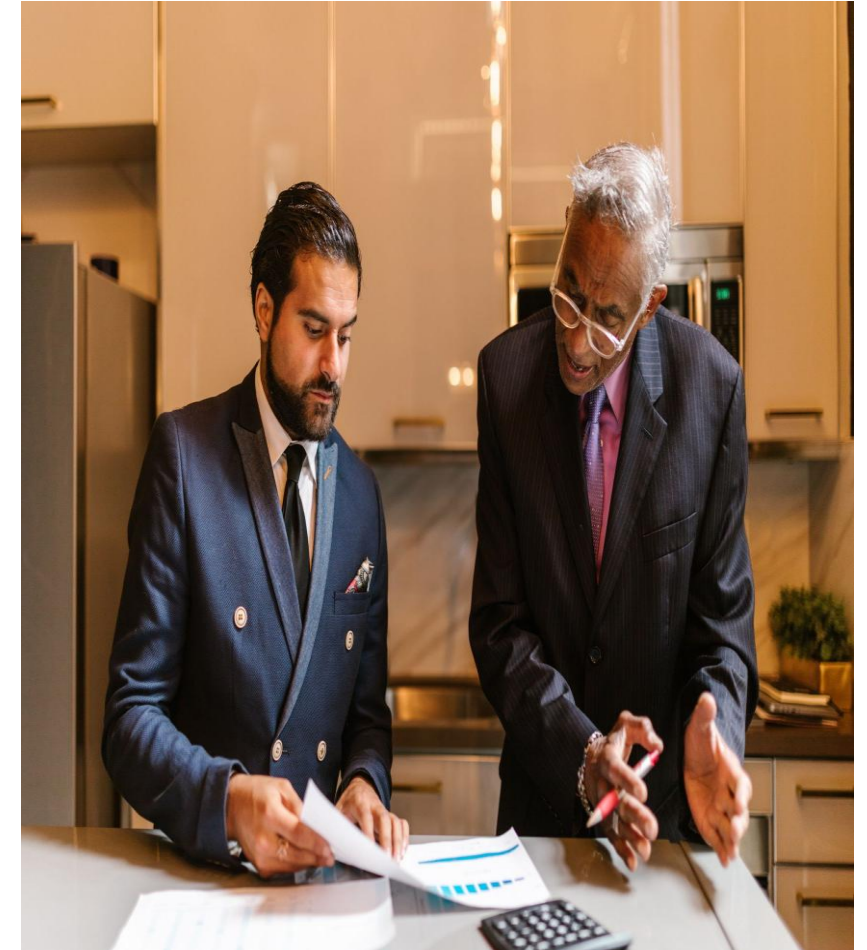
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Banking is digital, interconnected and closely supervised

Trust is the franchise—and the target

₹48,021 cr

Frauds reported by banks and FIs
in FY26 (RBI Annual Report)

6 hours

To report cyber incidents to RBI
on DAKSH

29 banks

Using RBIH's MuleHunter.AI (July
2026)

31 Jul 2026

RBI's new cybersecurity
Directions for banks

What this means: banks must now show board-level governance, continuous monitoring, frequent testing and rapid reporting—under directions that took effect immediately on 31 July 2026.

Sources: RBI Annual Report 2025-26 (frauds of ₹1 lakh and above); Government reply to Parliament, July 2026; RBI Directions, 31 July 2026.

Who we serve across banking



Public sector banks

Large networks, legacy estates, government business



Private sector banks

Digital-first channels and rapid change



Foreign bank branches

Group standards with local obligations



Small finance banks

Inclusion-focused, digital growth, lean teams



Payments banks

Payments, deposits and digital interfaces



Urban co-operative banks

Graded requirements by digital depth



Rural banking

RRBs, StCBs and DCCBs supervised by NABARD



Banking technology providers

Core, switch, cloud and fintech partners

The threats that cost banks the most

Six priorities from our 18-threat banking assessment



Account takeover & mule accounts

SIM swap, OTP theft and rented accounts move fraud proceeds fast



Ransomware

Encrypted branches and channels, deleted backups, extortion



Third-party & ATM switch

Shared service providers become a route into the bank



Phishing, vishing & deepfakes

Impersonation of customers, staff and executives



API & digital channel attacks

Fintech and co-lending APIs that overshare data



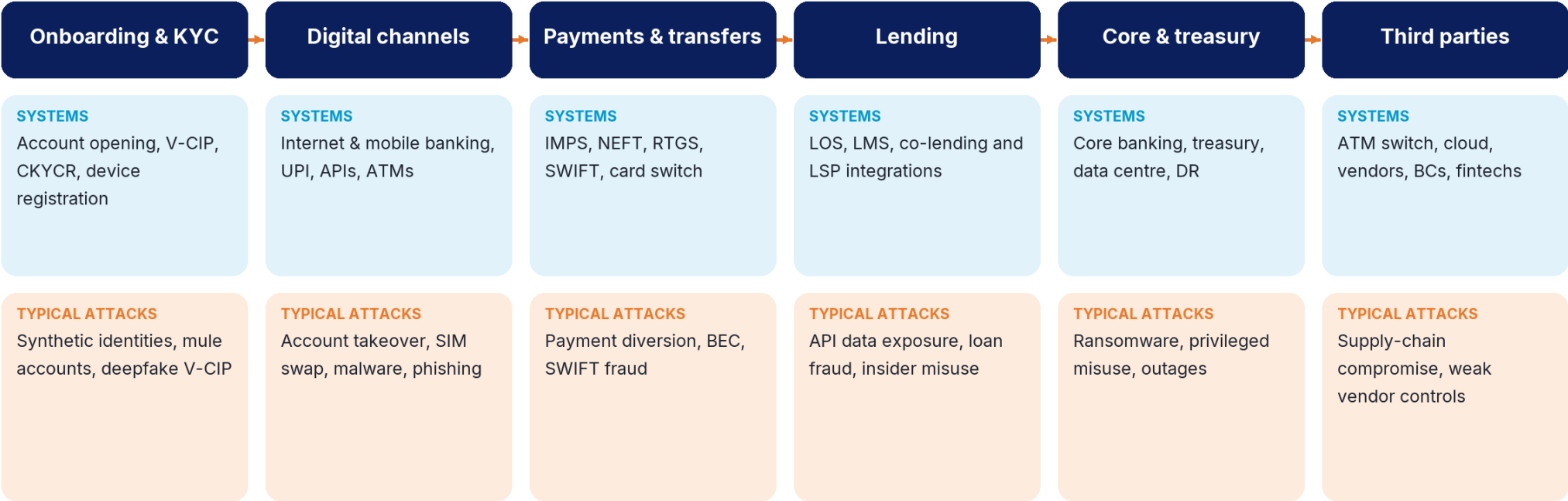
Slow detection & reporting

Missing logs and untested playbooks blow the 6-hour window

Attacks target every stage of the banking relationship

Where Cyber Risk Sits in Banking Operations

Each stage of a banking relationship has its own attack surface



Security must follow the customer and the money across channels, systems and partners—one strong control cannot compensate for a weak link elsewhere.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

A new cybersecurity rulebook for banks took effect on 31 July 2026

The 2026 rulebook—and the calendar it sets

Requirement	Frequency / deadline	Source
VA of critical and customer-facing DMZ systems	At least every six months	RBI 2026 Directions (commercial banks)
Penetration testing of the same systems	At least every 12 months	RBI 2026 Directions
Cyber incident reporting on DAKSH	Within 6 hours of detection	RBI 2026 Directions; CERT-In (6 hours)
DR drills for critical systems	At least half-yearly, full working day on DR	RBI 2026 Directions
IT Strategy Committee meetings	At least quarterly	RBI 2026 Directions
CISO cyber risk review to Board/RMC/ITSC	At least quarterly	RBI 2026 Directions
Two-factor authentication with a dynamic factor	In force from 1 Apr 2026	RBI Authentication Directions
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 Banking Cybersecurity

Key Indian instruments that shape bank cybersecurity, audit and assurance

● In force ● Upcoming (from Oct 2026)

Apr 2018	● RBI: Storage of Payment System Data (data localisation for payment data)
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
Nov 2025	● RBI consolidates instructions into 244 Master Directions; DPD Rules notified
Apr 2026	● RBI Authentication Directions in force: two factors, one dynamic
Jun 2026	● RBI issues revised customer-protection framework for fraudulent transactions
Jul 2026	● RBI Cybersecurity, Technology Risk, Resilience & Assurance Directions for banks
Jan 2027	● Revised customer-protection framework applies to transactions from this date
May 2027	● Most DPD Rules obligations, incl. breach intimation, take effect

Sources: RBI, CERT-In, MeitY official notifications. Applicability depends on bank category.

How Codec Networks helps

Regulatory assurance · VAPT · SOC · Resilience

One partner across every banking channel



Regulatory Assurance

Gap assessments against RBI's 2026 Directions, IS audit support, PCI DSS and SWIFT CSP



VAPT & AppSec

Six-monthly VA, annual PT, internet, mobile banking and API testing



24/7 Cyber SOC

CSOC with L1–L3 analysts, SIEM, EDR/XDR, fraud and mule signals



Cyber Resilience

Ransomware readiness, backup tests, DR drills, crisis management plan



Forensics & Response

Triage, evidence, 6-hour reporting support, fraud investigations



Third-Party & Privacy

ATM switch, cloud and fintech partner reviews; DPDPA readiness

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

Co-operative banks, smaller SFBs and banks building a baseline

- Scoped VAPT and retest (B1)
- Gap review against RBI directions (B4)
- Backup and DR readiness check (B10)
- Risk register and roadmap (B5)

Assurance

Mid-sized private banks, SFBs and payments banks

- Six-monthly VA, annual PT (B1)
- Digital channel and API testing (B2)
- Regulatory evidence pack (B4)
- Extended-hours SOC + IR (B7, B8)

Continuous Resilience

Large public and private sector banks

- Red teaming and simulations (B1, B10)
- Third-party and ATM switch assurance (B9)
- 24x7 CSOC with L1–L3 (B7)
- Quarterly Board and ITSC reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
VA at least six-monthly and PT at least annually for critical and customer-facing DMZ systems (RBI 2026 Directions)	Scheduled VA/PT by independent experts, with retest	B1
Application security testing across the lifecycle; source code or escrow for critical applications	Secure code review, application and API testing	B2
CSOC with 24x7 Level 1 monitoring; anti-phishing and anti-rogue-app services	Managed CSOC and brand monitoring	B7
Cyber incidents reported to RBI on DAKSH within 6 hours; CERT-In notified	IR retainer, playbooks and reporting support	B7, B8
DR drills for critical systems at least half-yearly; BCP/DR reviewed annually by the ITSC	DR drill observation, ransomware simulation	B1, B10
Baseline controls for ATM switch providers and third-party IT arrangements	Third-party and ATM switch provider assessments	B9
DLP, data governance and DPDP safeguards	DPDPA programme, data-flow mapping, DLP review	B6

Five new case studies, five broken chains

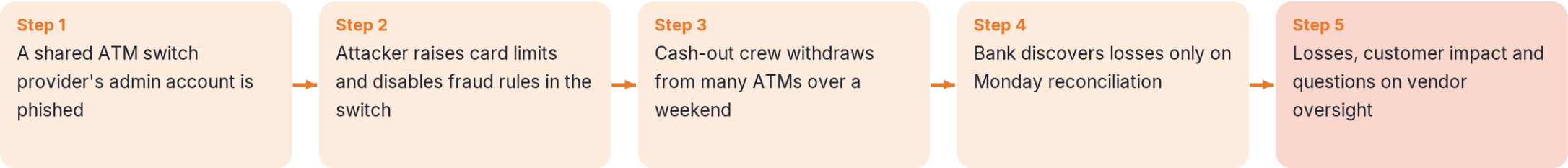
Illustrative composite scenarios written for 2026—not client engagements

1	The Mule Network Hiding in Plain Sight	Rented and synthetic accounts move scam money; risk scoring and velocity rules expose them	B7 · B8 · B4
2	The ATM Switch That Was Someone Else's Problem	A shared switch provider is phished; contractual controls and limit alerts stop the cash-out	B9 · B7 · B3
3	Ransomware on a Friday Night	Branches go dark; EDR, isolated backups and a rehearsed crisis plan limit the damage	B7 · B10 · B8
4	The Fintech API That Overshared	A partner API leaks KYC data; minimisation, secrets scanning and API monitoring prevent it	B2 · B9 · B6
5	The CEO's Voice on the Phone	A cloned voice approves a transfer; call-back and maker-checker controls break the chain	B10 · B7 · B5

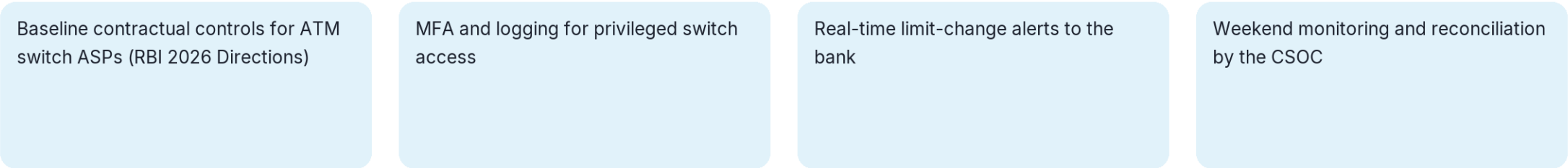
Example: breaking an ATM switch cash-out chain

Case 2: The ATM Switch That Was Someone Else's Problem

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: privileged access and MFA at the switch provider, the contractual baseline controls RBI's 2026 Directions require for ATM switch providers, and whether limit changes trigger real-time alerts to the bank's CSOC.

Why banks choose Codec Networks



CERT-In empanelled

For information security auditing services; NISAP empanelled for application audits



Certified

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



Regulation-mapped

Mapped to RBI's 2026 Directions, CERT-In, DPDP, PCI DSS and SWIFT CSP



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

Bank category, channels, critical systems, third parties and your inspection 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.