NBFC Cyberattacks: 12 Firms Lose Over Rs 65 Crore in Three Months in Delhi-NCR



Original symbolic graphic: pcsmantra.com

Why in News

According to the Indian Express (16 November 2026), **12 non-banking financial companies (NBFCs)** in Delhi-NCR lost **over Rs 65 crore to cyber fraud in the past three months**. Police say attackers exploited weaknesses in the companies' **payout APIs** - the payment rails through which loans are disbursed and payments move at scale. Meanwhile, the **Telangana Cyber Security Bureau (TGCSB)** has warned of AI-assisted cyberattacks on payment systems, and recent international raids have exposed transnational fraud networks targeting India's lenders.

Key Facts

- **Scale:** 12 NBFCs in Delhi-NCR, Rs 65 crore+ lost in three months (IE report citing police sources).
- **Method:** exploiting payout API vulnerabilities; misuse of insider/external access credentials; layering of funds across multiple accounts and wallets.
- **New threat:** TGCSB warns generative AI is upgrading phishing, deepfake calls and automated social engineering.
- **Enforcement:** coordinated international raids (ToI) have uncovered transborder call-centre and fraud networks.

Regulatory Framework

- **Who regulates NBFCs:** the Reserve Bank of India - registration, prudential norms and IT governance; for Top, Upper and Middle Layer NBFCs, the RBI's **Master Direction on IT Governance (2023)** mandates a cyber-security framework, incident reporting and board-level oversight.
- **Legal basis:** Information Technology Act, 2000 (Section 43A - protection of sensitive data; Section 66 - computer-related offences), plus cheating provisions of the IPC/BNS.
- **Data protection:** The DPDP Act's section 8 security and breach-notification duties are in the 18-month commencement tranche and are not yet in force on 16 November 2026. CERT-In directions make reporting of specified cyber incidents **mandatory within 6 hours**.

Why It Matters

- **Financial stability (GS-3):** NBFCs are the backbone of small-ticket lending and last-mile credit; attacks on them hurt financial inclusion and customer trust alike.
- **Cyber security:** in an API-driven stack, perimeter security is inadequate; zero-trust architecture, strong authentication and real-time fraud monitoring are essential.
- **AI's dual nature:** AI strengthens both defence and offence - policy must account for both.

Prelims Practice Questions

Q1. NBFCs are primarily registered and regulated by:

(a) SEBI

(b) RBI

(c) IRDAI

(d) Ministry of Finance directly

Answer and Explanation

Answer: (b) NBFCs are registered with the RBI under Section 45-IA of the RBI Act, 1934 and bound by its prudential and IT directions.

Q2. Under CERT-In directions, specified cyber incidents must be reported within:

(a) 24 hours

(b) 72 hours

(c) 6 hours

(d) 48 hours

Answer and Explanation

Answer: (c) CERT-In's 2022 directions mandate reporting of specified cyber incidents within 6 hours of noticing them.

Mains Practice Question

Q: "Digital finance cannot scale sustainably without a parallel scaling of cyber-risk management." Discuss in the context of rising cyber fraud in the NBFC sector and suggest regulatory and technical measures. (250 words)

Outline: Introduction - the latest NBFC fraud figures; risk dimensions - API vulnerabilities, AI-driven attacks, data breaches; regulatory framework - RBI IT governance, CERT-In, DPDP; measures - zero-trust, MFA, fraud analytics, staff training, international cooperation; conclusion - trust is the currency of digital finance.

FAQ

Short answer: Twelve NBFCs in Delhi-NCR lost over Rs 65 crore to cyber fraud in three months; attackers targeted payout APIs. RBI IT governance directions apply to Top, Upper and Middle Layer NBFCs; CERT-In's separate 6-hour reporting rule applies. The DPDP Act's section 8 security and breach-notification duties are in the 18-month commencement tranche and are not yet in force on 16 November 2026. TGCSB has warned of AI-assisted attacks.

Q: How are NBFCs being attacked?

Police say attackers exploit payout API weaknesses and misuse credentials to layer loan-disbursement and payment funds across accounts; TGCSB notes a growing role for AI-based phishing and deepfakes.

Q: Which cyber-security rules apply to NBFCs?

For Top, Upper and Middle Layer NBFCs, the RBI's Master Direction on IT Governance (2023) mandates cyber frameworks and incident reporting; a 6-hour report to CERT-In; The DPDP Act's section 8 security and breach-notification duties are in the 18-month commencement tranche and are not yet in force on 16 November 2026. and penal provisions of the IT Act, 2000.

Q: What precautions should customers and companies take?

Companies: API security audits, multi-factor authentication, real-time fraud monitoring, staff training. Customers: never share OTPs/passwords, avoid unknown links, report suspicious transactions immediately (1930 helpline / cybercrime.gov.in).

Sources

- Indian Express (16 November 2026): 12 NBFCs lose Rs 65 crore in three months in Delhi-NCR
- Times of India (Hyderabad): international raids - payout APIs turned into theft routes
- The Hindu: TGCSB warns NBFCs and fintech firms of AI-assisted cyberattacks
- Note: no official data release was located for this story; figures are from police/TGCSB sources as quoted in the reports above