DIGITAL FINANCIAL FRAUDS IN INDIA - GS III MAINS

Q. Discuss the reasons for the surge in recent instances of digital financial frauds across India. Also, bring out the measures taken by the government to address the frauds. (15 marks, 250 word)

News: *Digital financial frauds in India: a call for improved investigation strategies*

What's in the news?

- A recent report by the Indian Cyber Crime Coordination Centre revealed that digital financial frauds accounted for a staggering ₹1.25 lakh crore over the last three years.

Key takeaways:

- According to the National Crime Records Bureau (NCRB), cybercrimes in India in 2023 resulted in a staggering loss of ₹66.66 crore, with 4,850 reported cases.
- A recent report by the Indian Cyber Crime Coordination Centre (I4C) revealed that digital financial frauds accounted for a staggering ₹1.25 lakh crore over the last three years.
- According to the National Cybercrime Reporting Portal (NCRP), in 2023, at least ₹10,319 crore was reported to be lost by victims of digital financial fraud.
- According to the report, the number of complaints received in 2023 alone was 6.94 lakh.

Digital Financial Frauds:

- It encompasses a spectrum of illicit activities targeting online or mobile banking systems.
- These activities include the theft of personal information, unauthorized access and fraudulent transactions.
- As fraudsters continually refine their tactics, employing sophisticated methods like phishing, malware and social engineering attacks, the challenges for both individuals and financial institutions in detecting and preventing these activities become increasingly complex.

Working of Digital Financial Frauds:

- Convincing the victim to send money, either by impersonation (fake WhatsApp/FB/Insta, social media profiles) or by giving them a fake promise of higher return.
- By taking credentials including Unified Payments Interface ID (UPI), Personal Identification Number (PIN), One-Time Password (OTP) or Internet banking ID/password from the victim and then the use of the same on different apps/websites and shifting cash without the knowledge of the victim.
- By taking card information and convincing the victim to share OTP.

Reasons for Rise in Digital Financial Frauds:

1. Technology Advancement:

a. Online Banking Risks:

- The convenience of online banking introduces risks such as phishing attacks, account takeover fraud and malware. Robust authentication measures, including biometric authentication, emerge as imperative safeguards.

b. Mobile Banking Vulnerabilities:

- While mobile banking offers unparalleled ease, it is more susceptible to online fraud.
- Strengthening authentication protocols and educating users on securing their devices become indispensable measures.

c. ATM Vulnerability:

- Despite their convenience, ATMs are susceptible to skimming and hacking. Regular maintenance, transaction monitoring and education play pivotal roles in combating ATM fraud.

d. Digital Payment System Risks:

- Digital payment systems provide convenience but also open new avenues for exploitation by fraudsters.

2. Weak Anti-fraud Measures:

a. Lack of Strong Authentication Protocols:

- Many online banking systems rely on weak authentication, rendering them vulnerable to attacks.
- The implementation of biometric authentication and multi-factor authentication (MFA) emerges as a critical defence.

b. Use of Weak Passwords:

- Easily guessed weak passwords leave accounts vulnerable. Strategies such as two-factor authentication (2FA) significantly enhance security.

c. Phishing and Social Engineering:

- Exploiting human emotions through phishing attacks and social engineering tactics remains a persistent threat.

3. Lack of Regulatory Compliance:

a. Compliance challenges:

- Financial institutions grapple with staying abreast of evolving regulatory requirements, leading to vulnerabilities.

b. Consequences of Non-Compliance:

- Non-compliance may result in severe consequences, including hefty fines and reputational damage.

4. Increasing Sophistication of Fraudsters:

a. Use of Advanced Technology:

- Fraudsters leverage advanced technology, including AI and machine learning, making detection increasingly challenging.

b. Collaborative Fraud Networks:

- Collaboration among fraudsters complicates prevention efforts.

5. Insider Threats:

a. Employee Negligence:

- Employee negligence can expose sensitive information, necessitating regular training and audits.

b. Employee Misconduct:

- Strict internal controls and regular audits are essential to prevent employee misconduct.

c. Third-party Risks:

- Third-party vendors pose risks if they lack adequate security measures, emphasizing the need for regular audits.

Government Initiatives:

1. Digital Intelligence Platform (DIP):

- It is an initiative evolved by the Department of Telecommunications to function as a strong and incorporated platform for real-time intelligence sharing, information exchange and coordination amongst diverse stakeholders.

2. Chakshu Facility:

- It is a newly introduced function at the Sanchar Saathi portal that encourages residents to proactively record suspected fraudulent communications acquired by call, SMS, or WhatsApp.

3. National Cyber Crime Reporting Portal:

- It aims to enable complainants to report lawsuits concerning all types of cybercrimes, which include internet and online frauds.

4. Role of RBI:

- Reserve Bank of India has issued several circulars/guidelines related to security and risk mitigation measures for securing electronic/digital payment transactions.

- The government and RBI has blocked 1.4 lakh mobile numbers so far that were involved in financial frauds.

5. Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS):

- It aims to onboard banks and financial institutions on the platform through API integration.
- Integration of CFCFRMS platform with the National Cybercrime Reporting Portal (NCRP) to centralise the platform that will enable effective collaboration between Police, Banks and Financial Institutions, allowing for real-time monitoring and prevention of fraudulent activities

WAY FORWARD:

1. Filters for Higher Transactions:

- Implementation of mandatory filters for transactions above a certain monetary threshold. This includes the use of one-time passwords (OTP) for digital payments. The aim is to enhance security and prevent fraudulent transactions.
- The government is also exploring the creation of intelligence within payment systems to identify and block suspicious activities.

2. Awareness Generation:

- It is the need of the hour is to increase awareness among customers on how to secure their bank accounts and UPI IDs.
- Banks are likely to be urged to renew awareness and education efforts on cyber fraud prevention mechanisms for customers.
- There is also a need to have more stringent screening of junk or spam calls by fraudsters.

The fintech and telecom industries should be mandated to take certain preventive steps in their technology and offer statistics in a manner which enables quicker investigation, the prevention, detection, recuperation and conviction will be much more effective. Faster availability of data will make it simpler to be aware of and convict pan-Indian gangs.