Reforms for Secure Digital Connectivity

For Prelims: Reforms for Secure Digital Connectivity, Digital Ecosystem, Know Your Customer, Point of Sale (POS), World Telecommunication Day.

For Mains: Reforms for Secure Digital Connectivity.

Source: PIB

Why in News?

In order to promote Safe Telecom Utilisation, the government has introduced two reforms for mobile user protection to **promote a cleaner and safer** Digital Ecosystem.

- The two reforms, KYC (Know Your Customer) **Reforms and** Point of Sale (POS) **registration Reform**. These two reforms are in the direction of earlier reforms introduced with the launch of **Sanchar Saathi,** a citizen-centric portal that has empowered India's fight against the menace of cybercrimes and financial frauds.

What are the Reforms?

- **KYC Reforms**: KYC reforms play a pivotal role in safeguarding subscribers of telecom services from potential frauds and bolstering public confidence in the digital ecosystem.
    - **QR Code Scanning of Aadhaar:** To prevent misuse of printed **Aadhaar,** demographic details are captured by scanning the QR code of printed Aadhaar during the KYC process.
    - **Mobile Number Disconnection:** Disconnected mobile numbers will not be allocated to new customers for 90 days after disconnection, preventing immediate reuse.
    - **Complete KYC for SIM Replacement:** Subscribers must complete KYC when replacing their SIM cards.
    - **Biometric Authentication:** In addition to thumbprints and iris-based authentication, facial-based biometric authentication is permitted in Aadhaar E-KYC.
    - **Business Connections:** Entities such as companies, organizations, trusts, and societies can obtain mobile connections after completing KYC for all end-users. Activation occurs only after successful KYC and physical verification of the entity's premises.
- **Point-of-Sale (POS) Registration Reforms:** This reform aims to ensure the integrity of the distribution network by mandatorily registering Franchisees, Agents, and Distributors (PoS).
    - The process involves **robust verification and written agreements** between PoS and Licensees. Any PoS engaged in **illegal activities will be terminated and blacklisted for three years.**

What is the Sanchar Saathi Portal?

- **About:**
    - The **Sanchar Saathi portal**, developed by the **Centre for Development of Telematics (C-DOT)** under the **Department of Telecommunications (DoT)**, is revolutionizing the

    telecom sector in India.
    - It was launched on **World Telecommunication Day** (17th May 2023).
- **Objective:**
    - The primary objective of the Sanchar Saathi portal is to address various **fraudulent activities** prevalent in the telecom industry, such as **identity theft, forged KYC, and banking fraud.**
        - By leveraging advanced technologies and frameworks, the portal aims to provide users with a secure and trustworthy telecommunication experience.
- **Reforms Introduced:**
    - **CEIR (Central Equipment Identity Register):**
        - Implemented to **block stolen or lost mobile phones.**
        - Users can submit **IMEI numbers** along with a copy of the police complaint to verify and block stolen devices.
        - Integrated with Telecom Service Providers and Law Enforcement Agencies.
        - **Prevents stolen devices from being used in Indian networks** and allows tracing by law enforcement when necessary.
    - **Know Your Mobile Connections:**
        - Allows users to **check mobile connections registered in their name.**
        - Enables **identification of unauthorized or fraudulent connections.**
        - Users can report fraudulent or unrequired connections, triggering **re-verification and termination of reported connections.**
    - **ASTR (**Artificial Intelligence **and** Facial Recognition **powered Solution for Telecom SIM Subscriber Verification):**
        - Developed to identify **subscribers who obtain connections using fraudulent or forged documents.**
        - Utilizes f**acial recognition and data analytics** techniques.
        - Analyzes connections obtained through **paper-based KYC documents.**
- **Impact:**
    - Over 40 lakh fraudulent connections were identified and over 36 lakh were disconnected using the portal.
    - Provides a secure and trustworthy telecommunication experience for users.
    - Protects against identity theft, forged KYC, mobile device theft, and banking fraud.

Conclusion

- By introducing comprehensive reforms and harnessing technological tools like the **'Sanchar Saathi' portal and ASTR**, the department has effectively identified and acted against fraudulent activities.
- This approach aligns with the government's mission to provide a secure and reliable communication environment for all citizens.

PDF Refernece URL: https://www.drishtiias.com/printpdf/reforms-for-secure-digital-connectivity