**India’s e-Zero FIR Reform: A Digital Leap Toward Accessible Justice**

***Submitted by: Rasveen Kaur Kapoor, practicing advocate at the Delhi High Court***

In a significant development for India's legal and technological landscape, the Union Home Ministry's recent notification on the e-Zero FIR initiative marks a notable step forward in the digitisation of and access to justice for cybercrime victims. Initially launched as a pilot project in Delhi, the initiative aims to assess the system’s efficacy before a nationwide rollout. The e-Zero FIR is an electronic adaptation of the Zero FIR mechanism, rooted in Sections 173(1) and 173(1)(ii) of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). According to Union Home Minister Amit Shah, *“Launched as a pilot project for Delhi, the new system will automatically convert cyber financial crimes filed at NCRP or 1930 to FIRs, initially above the threshold limit of Rs 10 lakh. The new system, which will drive investigations swiftly cracking down on cybercriminals, will soon be extended to the entire nation,”* he stated on X (formerly Twitter). While this initiative holds genuine transformative potential, its effective implementation will require ongoing evaluation, legal scrutiny, and equitable expansion.

The e-Zero FIR pilot project currently active in Delhi is supposed to seamlessly convert complaints of financial cybercrime over INR10 lakh into First Information Reports (FIRs) via data pipelines connecting between the e-FIR platform operated by Delhi Police and the Crime and Criminal Tracking Network & Systems (CCTNS) at the National Crime Records Bureau (NCRB). This infrastructure fills a long-standing gap caused by discretionary delays in registering FIRs; an underlying issue which has been repeatedly flagged by the Courts. The Supreme Court and various High Courts have stressed the police's obligation to register FIRs without exception in matters of cognisable offence. The e-Zero FIR system supports this mandate in both spirit and function. In principle and design, the initiative is revolutionary. By implementing the Zero FIR concept which allows a police station to register a cognisable offence regardless of territorial jurisdiction; the government seems to fulfil two crucial promises: **accessibility** and **accountability**. Beyond speeding up FIR registration, the initiative facilitates early-stage evidence preservation which is vital in combating fast-moving cyber-financial crimes that often leave little digital trace if not acted upon swiftly. More importantly, this reform represents a clear shift in the burden of action; transferring it from the victim who is often a professional or a business on the losing side to the State. These victims have historically faced the dual hardship of financial loss and bureaucratic red tape. Typically, the additional burden of completing a rather complicated administrative process through a formal route that seems to obscure action rather than facilitate it.

Nevertheless, the current structure of the initiative has its own set of limitations which needs to be acknowledged. The INR 10 lakh cap, while a judicious ceiling for the pilot project automatically disqualifies a substantial majority of victims of cybercrime. Mid-level frauds in the range of INR 50,000 and INR 9,00,000 are neither insignificant nor infrequent. For most people and small enterprises, these figures amount to months of earnings or operating capital. A future revision of this threshold or its removal is necessary to ensure inclusivity and fairness. Further, there is also the issue of potential misuse. Automation minimizes the need for human judgment, which can be both a strength and a vulnerability. Without robust Standard Operating Procedures (SOPs), oversight mechanisms, and triage protocols, the system risks being misused through frivolous or malicious complaints thereby defeating its own purpose.

For the initiative to succeed on a national level, interoperability between States not just within Delhi must be prioritised. Uniformity in response, training for cybercrime cells, and synchronisation with digital payment systems (for fund freezing and tracing) is necessary. The e-Zero FIR’s strength lies in its vision: *a future where digital crimes meet a digital-first response*. By aligning jurisdiction-neutral policing with technological automation, it removes long-standing chokepoints in justice delivery. But to become a true equaliser, this tool must evolve into a national standard with broader inclusion, thoughtful safeguards, and vigilant implementation.