

Zero FIR in Cyber Offences:

A welcome step by the MHA to expedite action against cyber crime

28 May 2025

The Ministry for Home Affairs (MHA), Union of India, has recently announced a new initiative of the Indian Cybercrime Coordination Centre (I4C), which mandates converting any criminal complaint pertaining to a cyber offence, involving an amount more than INR 10,00,000 (initial limit), into a Zero First Information Report (FIR), immediately. This initiative has been taken in furtherance of the Government's drive to combat cyber-crime and is a welcome step towards ensuring expeditious action against cyber offences. A pilot version of the initiative has been launched in Delhi, and the full version of the initiative is soon expected to be adopted on a nation-wide basis.

Brief Background

The I4C was created under a special scheme of the MHA, which received approval in October 2018 and was formally launched in 2020. The I4C aims to tackle various issues pertaining to cyber-crime, while also researching on these issues and assisting law enforcement in improving their operations.

One of the 7 key components of the I4C is the National Cyber Crime Reporting Portal (NCRP), which is an online portal on which citizens can register complaints in relation to any cyber-crime incident. Citizens wishing to register a complaint over phone can call the NCRP's national helpline number – 1930.

The NCRP works as a centralized system where victims of cyber-crime can report offences committed against them in any part of India; the system after receiving the complaint automatically assigns the same to the concerned State / Union Territory, for taking appropriate action. The complaint is then allocated to the police station having jurisdiction, for inquiry and investigation. Citizens can trace the status of their complaints on the NCRP and receive information on the action taken, in real time.

The NCRP has many interesting features, such as providing a chatbot to answer queries and assist persons in filing complaints, maintaining a list of known cyber-offenders in order to caution the public against dealing with them, allowing public spirited individuals to register as volunteers in the drive against cyber-crime, etc.

The recent decision of the Government to allow prompt registration of Zero FIRs, where complaints are received by the NCRP (online or through the national phone helpline), will expedite investigation into cyber offences.

What is an FIR?

An FIR is an official public document created by the police to record the occurrence of a 'cognizable offence' i.e. an offence for which the police can arrest without a warrant (Section 154, Code of Criminal Procedure, 1973 / Section 173, Bharatiya Nagarik Suraksha Sanhita, 2023). An FIR captures the substance of the information received by the police, as also the name of accused persons, time and place of occurrence of offence, etc.

Ordinarily, victims of offences and/or persons wishing to register a complaint have to approach the concerned police station having territorial jurisdiction to investigate the concerned offence (determined basis the place where the offence was committed). The police, on receiving the complaint, may conduct a preliminary inquiry and then proceed to register an FIR (when, prima facie, the existence of a cognizable offence is made out). The investigation into an offence formally starts after registration of FIR.

What is a Zero FIR?

The concept of Zero FIRs was introduced by the Justice Verma Committee, constituted after the infamous Nirbhaya case in Delhi, to suggest changes in the criminal law system of the time. A Zero FIR can be registered by any police station on receiving knowledge of an offence, even if such police station does not have the territorial jurisdiction over the area where the offence was committed. The FIR is then transferred internally to the police station having jurisdiction, which then takes over the investigation. Considering the procedural burden which comes with this concept, Zero FIRs are only registered in select offences, which are of a sensitive nature, such as heinous offences (rape, murder etc.). The name 'Zero FIR' comes from the practice of not giving a specific number to such FIRs (and merely ascribing the number '0' to them); the FIR is given an actual number once it is transferred to and received by the appropriate police station.

Some of the key benefits of permitting Zero FIRs are as follows:

- i. Expedites the action to be taken against the offender, with the police being bound to initiate investigation;
- ii. Provides ease of access to the common man, who can approach any police station which may be conveniently located;
- iii. Helps with timely recording of the facts qua an offence, which may help in capturing key evidence.

Registration of Zero FIR in Cyber Offences

With this new initiative of the I4C, any complaint (above the prescribed financial threshold of INR 10,00,000) will be immediately converted into an FIR and then be transferred to the police station holding jurisdiction. The police would then be duty bound to investigate into the offence and maintain a case diary (recording the details of the investigation) and cannot delay taking action on the matter.

The police would also have the power to conduct arrest / search and seizure of premises, etc. which would enable an effective investigation.

Comments

This is a welcome step on part of the Government to encourage the police to act promptly when dealing with cyber offences. In such offences, it is often found that immediate action is key in preventing escape of cyber criminals and / or for the stolen property to be traced and recovered.

The police ordinarily have the power to delay registration of an FIR till they conduct a preliminary inquiry and /or even refuse to register an FIR, altogether. Practical instances of deliberate delay on part of the police are also seen frequently.

With the advent of this new initiative mandating Zero FIR registration, the inordinate delays in taking action against cyber-crime can be curbed. This is also in furtherance of the purpose of creating the I4C, and the NCRP under it.

This initiative is likely to benefit businesses (in addition to citizens), as it provides assurance of expeditious action when such businesses are targeted by cyber criminals, which can prevent major financial losses. At the same time, businesses having online operations and dealing with data (intermediaries) may anticipate receiving an increased number of police summons for information and assistance, as the number of cyber-crimes being investigated is likely to increase. Hence, it is pivotal for such intermediaries to take appropriate steps for ensuring continued compliance with relevant rules under the Information Technology Act, 2000 and providing full assistance to law enforcement agencies.

- Supratim Chakraborty (Partner) and Ishan Khanna (Counsel)



About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1200 legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com



This document has been created for informational purposes only. Neither Khaitan & Co nor any of its partners, associates or allied professionals shall be liable for any interpretation or accuracy of the information contained herein, including any errors or incompleteness. This document is intended for non-commercial use and for the general consumption of the reader, and should not be considered as legal advice or legal opinion of any form and may not be relied upon by any person for such purpose. It may not be quoted or referred to in any public document, or shown to, or filed with any government authority, agency or other official body.

www.khaitanco.com | © Khaitan & Co 2025 | All Rights Reserved.

Ahmedabad · Bengaluru · Chennai · Delhi-NCR · Kolkata · Mumbai · Pune · Singapore