



CYBER CRIME - INVESTIGATION GUIDELINES

CYBER CRIME CELL

No. /SP(Cyber)/2024

O/o the SP(Cyber Crime)
Puducherry

Date: 06.02.2024

As observed and directed by DIG, in Cyber Crime PS the criminal cases and complaints registered under NCRP Portal are pending investigation for long period. It was further sensitized that the **offence against women & Child** cases are more sensitive inviting attention of **"Fast Track"**.

Based on the above, periodical sensitization was being imported to all staffs and ascertained that IO / EO are keep on

1. Collecting data from social media / Telecom / Internet Service providers
2. Not able to arrange the case file / enquiry file
3. Hesitations to finalize the investigation / enquiry
4. Fear to prepare Final Report
5. No idea about the Investigation Check-list to finalize
6. Needy action on Social Media ID (Hacking / Fake creation).
7. Online Customer support automated system established by Social Media to support their customers
8. Action to be initiated directly by Customer through Helpline and action to be initiated by IO / EO as LEA (Law Enforcement Authority).
9. SOP / Code of Contact if any complaint on Hacking of Data Base / Servers etc where the attention of CERT-In & I4C / JCCT-6 is required or to be done by them.
10. Periodical data on fraudster Mobile / IMEI / IP / URL to be communicated to I4C / JCCT-6 for mapping and further action at India Level or Global Level.
11. Updating / Sensitizing complainant on the status of his complaint.

In order to create awareness on the above, this circular is prepared as guide cum check-list for the staffs of Cyber Crime Police Station / Cell to facilitate them to finalize the cases at the earliest or to seek the guidance of Senior Officers to boost the image of Puducherry Police



CYBER CRIME - INVESTIGATION GUIDELINES

INVESTIGATION CHECKLIST

Complaint on SOCIAL MEDIA ABUSE / MISUSE

1. FIR / NCRP Registration
2. Complaint copy
3. **65-B Certificate** on the screen prints for proof of crime.

INVESTIGATION

4. **Identifying route of crime**
 - A. Mobile number utilized
 - B. Social Media ID posted the abusive content
 - C. URL link for the posting with time stamp
 - D. URL link for web application for online challenges
5. **Data request from Service Providers**
 - A. Social Media - (Instagram / Facebook, Telegram / X / Whatsapp, etc.)
 - B. Internet / Telecommunication - (ISP / TSP)
 - C. Website @ URL (link) posting to the abusive content.
6. **Receipt of reports** from Social Media Service Provider.
7. **Letter to I4C** for blocking fraudster Website @ URL (link)
8. **Letter to Service Provider** for block Mobile / IMEI / User ID
9. **Findings**
 - a) Abusive content Social Media IP address mapping service provider for Internet and its corresponding IP mapping to accused & his location.
 - b) **If required, go for Corroborative above Evidence**
 - Mapping Mobile number (GPS mapping to accused & his location)
 - Mapping E-mail log IP
 - Mapping Email linked (e-mail & mobile)
10. Statement of the complaint / Witnesses.
11. List of Documentary evidence.
12. Memo of evidence



CYBER CRIME - INVESTIGATION GUIDELINES

INVESTIGATION CHECKLIST

ONLINE FINANCIAL FRAUD

1. FIR / NCRP Registration
2. Complaint copy
3. Complainant payment details with time stamping
4. Accused Account details & Website address
5. **65-B Certificate** on the screen prints for proof of crime.

INVESTIGATION

6. **GO through the SOP issued by DIG.**
7. **Identifying route of crime**
 - A. Mobile number utilized
 - B. Social media posted the abusive content
 - C. URL link for the posting with time stamp
 - D. URL link for web application for online challenges
8. Transaction details from the accused account obtained from NCRP Portal
 - A. Layer 1 - Accused account
 - B. Layer 2 - Amount disposal from accused account
 - C. Layer 3 - Further transaction
 - D. Layer 4 - Further transactions
9. **Data request from Service Providers**
 - A. Bank account KYC of the fraudster / Accused
 - B. Transaction details and account balance
 - C. Social media - (Instagram / Facebook, Telegram / X / Whatsap, etc.)
 - D. Internet / Telecommunication - (ISP / TSP)
 - E. Website @ URL (link) posting to the abusive content.
10. **Receipt of reports** from Social Media Service Provider.
11. **Blocking**
 - A. **Letter to Banks to block / Lean mark the fraudster accounts**
 - B. **Letter to I4C for blocking fraudster Website @ URL (link)**
 - C. **Letter to Service Provider for block Mobile / IMEI / User ID**
12. **Tracking accused**
 - A. Mapping of IPs from Bank transactions / Social media contacts
 - B. Its corresponding IP mapping to accused & his location.
 - C. **If required, go for Corroborative above Evidence**
 - Mapping Mobile number (GPS mapping to accused & his location)
 - Mapping E-mail log IP & its linked mobile)
13. Statement of the complaint / Witnesses.
14. List of Documentary evidence
15. Memo of evidence



CYBER CRIME - INVESTIGATION GUIDELINES

INVESTIGATION CHECKLIST

Steps on Financial Fraud Cases for recovery of available amounts

Part - 1

1. Registering complaint in NCRP portal
2. Portal will provide Transaction details of the victim money to Fraudster Account and subsequent transaction to other accounts.
3. Transaction from Fraudster Account is Layer 1.
4. Subsequent transaction is Layer 2, then Layer 3

Part - 2

1. IO / EO should request **respective bank** to freeze the accounts and to verify the account holder KYC.
2. With clear KYC, if any one claims to unfreeze his account, then it has to be examined as to the genuineness of the transaction and his business. If satisfied then, as per SOP issued by DIG, the account can be recommended for unfreeze after **LEAN marking** the victim amount.

Part - 3

1. Upon satisfaction of **freezing of accounts in synchronization with the complaint**, IO / EO shall report before the respective **jurisdictional court** with FIR or NCRP
2. Or Shall request the complainant to file a petition before the respective **jurisdictional court** with FIR or NCRP
3. Guide the complainant to claim the balance amount through "Civil compensation"



CYBER CRIME - INVESTIGATION GUIDELINES

Social Media - FAKE ID

1. Assisting the **user @ victim** to use the Grievance Redressal Mechanism by the Service Provider to their customers.
2. Making the **user @ victim**
 - a) Login to the fake facebook.
 - b) Search the Fake ID.
 - c) Report fake ID as fake.

Social Media - HACKING

1. Assisting the **user @ victim** to use the Grievance Redressal Mechanism by the Service Provider to their customers.
2. Making the **user @ victim**
 - a) Login on to the service provider.
 - b) Help.
 - c) Report.
 - d) Follow the instructions to recover the account.

Social Media - Removal of Abusive Contents & tracing of Accused

1. Complaint to be registered in the NCRP Portal or FIR
 - A. Complaint copy
 - B. **65-B Certificate** on the screen prints for proof of crime.
2. Letter to Service Provider from Nodal Officer nominated by Police Department through official email ID.

Social Media - Tracing of Accused

1. KYC details & IP for abusive content posting to be obtained from Service Provider (FB / Whatsapp / Twitter / Instagram / Telegram)
2. ISP / TSP for the IP traced to be identified
3. KYC for the **IP with time stamp** to be obtained from ISP/TSP reaching accused
4. Brief history of the case - Connection between Victim & Accused, if any.

Attack on Website & Data Server (Hacking)

1. Report complaint to CERT-In
2. Information to Cyber Crime PS & IT / NIC as per SOP (I4C / CERT-In)



CYBER CRIME - INVESTIGATION GUIDELINES

ARRANGING OF CASE FILES

A. Direct FIR cases

1. Original FIR & Original complaint sent to court
2. FIR & Complaint copy
3. First CD
 - A. Rough work sheet of the IO
 - B. Statement of the Complainant & Victim
 - C. Statement of other witnesses
 - D. Crime Details Form
 - E. Documentary evidences including NCRP portal findings
 - F. Request sent
 - G. Reports received
 - H. Other
4. Second CD
 - A. Rough work sheet of the IO
 - B. Statement of the Complainant & Victim
 - C. Statement of other witnesses
 - D. Crime Details Form
 - E. Documentary evidences including NCRP portal findings
 - F. Request sent
 - G. Reports received
 - H. Other
5. Continue

B. FIR after NCRP investigation

1. Original FIR & Original complaint sent to court
2. FIR & Complaint copy
3. First CD
 - a) NCRP investigation details (entire file)
 - b) Statement of the Complainant & Victim
 - c) Statement of other witnesses
 - d) Crime Details Form
 - e) Documentary evidences including NCRP portal findings
 - f) Request sent
 - g) Reports received
 - h) Other



CYBER CRIME - INVESTIGATION GUIDELINES

Final Report - (Linking Crime & Criminal)

(Charge Sheet / Action Drop / MF / etc)

The IO / EO should focus on connection Crime & Criminal with evidence collected. It is sensitized not to keep-on collecting data and getting diverted for no use. In cyber-Crime, every complaint relies on **URL / weblink / IP** to prove the **Offence Committed**. This **URL / weblink / IP** proves the **SOC & accused location**. Periodically update the **List of documents / Memo of Evidence** as tabled below and prepare the Final Report (Charge Sheet, Action Drop, Mistake of Facts etc.)

LIST OF DOCUMENTS

1. FIR
2. Original Complaint
3. Supporting documents received from complainant with 65 B Certification
4. Statement of Witnesses
5. Requests sent and replies received
6. If data procured from computer, then 65 B Certificate for it
7. Pen Drives, SSD's, Hard disk's, etc., if any
- 8.

MEMO OF EVIDENCE

SN	Name and Address	Evidence
1	Complainant	Occurrence, lodging of complaint, submission of documents and other related facts
2	IO / EO	To Speak about registration of FIR, investigation and other facts
3	Nodal Officer / Manager etc.,	To speak about Bank Statement, CDR, CAF, IPDR etc., and connected facts.

1. Charge Sheet:

It is nothing but reproducing the DOR @ Gist of the offence, using words from the Section of Law added with accused name. Refer complaint brief in DOR and section of law connected with FIR / NCRP booked

2. Final Report (Action Drop, Mistake of Facts etc.):

This report generally restricted to 4 or 5 paras.

- A. Para-1. Reproducing the DOR @ Gist of the offence
- B. Para-2. Brief on the Investigation so far conducted
- C. Para-3. Views of the IO and reason there on for action drop treating the investigation finding as No Useful clues or Mistake of fact or etc
- D. Para-4. Requesting court to consider the facts in issue and to treat the investigation as AD / MF / etc and seeking to issue Slip Proceedings.

Dr. S. BASCARANE, PPS
SP (Cyber / Wireless / CCYNS / WIM)
Puducherry