Judicial Academy Jharkhand

झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सब के लिए
JHARKHAND STATE LEGAL SERVICES AUTHORITY
ACCESS TO JUSTICE FOR ALL

Standard Operating Procedure For

CYBER CRIME INVESTIGATION

STANDARD OPERATING PROCEDURE FOR CYBER CRIME INVESTIGATION

Description 1

❋ TYPES OF CYBER CRIME

Cyber crime may be said to be those where either the computer is an object or subject of the act constituting crime including conventional crimes. Broadly speaking any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crime comes within the ambit of cyber crime. Section 66 of the Information Technology (Amendment) Act 2008, defining cyber crime, refers to punishment if the acts detailed in Section 43 of Information Technology Act 2000, are done dishonestly or fraudulently.

Cyber crime can be categorized as 1. Crime against property, 2. Crime against Government 3. Crime against person

1. Crime against property

➢ **FINANCIAL FRAUD**

(Under IPC and Section 66 of IT Act)

➢ Financial fraud - These frauds include commercial fraud, investment fraud, hiring for jobs abroad etc by use of computer.

- Fraudulent or dishonest use of computer and computer resource to commit crime against property
  - Vishing fraud- Dishonestly or fraudulently misappropriating property using voice as a mean to extract private financial information like credit/debit / internet banking details
  - Job scams -Dishonestly or fraudulently misappropriating property using spoof emails, creating fake websites.
  - Social media fraud – Dishonestly or fraudulently misappropriating property by creating fake account on social media or through honey trapping.
  - Intellectual Property Crimes: Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc
  - Salami attack :Also known as salami slicing ,where a series of small fraud done on a regular basis through computer network/resources that finally adds up to a bigger fraud. For example a bank employee deducting a small sum of money daily from various customer's account which finally adds up to a large sum
- **DATA MODIFICATION**

(Under Section 66 of the Information Technology Act, 2000 and under Sections 403, 420,467, 406, 408, 409 etc of the Indian Penal Code, 1860) In this offence, the accused by accessing the Computer System, changes or damages the existing data/information or by doing any act mentioned in Section 43 of the IT Act fraudulently or with dishonest intention, and thereby causes harm to the person or to the institution.

2. Crime against person

IDENTITY THEFT

(Under Section 66C and 66D of the Information Technology Act, 2000)

- **Identity Theft and Impersonation**
  - **IDENTITY THEFT :-** Identity theft may be categorized as a crime against property or the crime against person. It is the fraudulent or dishonest use of electronic signature,password or unique identification of any person to commit Cyber Crime e.g seeking financial information of any person though vishing ,e-mail spoofing and causing misappropriation of property.
  - ***(Section 66C of IT Act deals with Punishment for identity theft.)***
  - **IMPERSONATION :-** A person to said to commit an act of personation if he cheats by pretending to be some other person ,or by knowingly substituting one person for another,or representing that he or any other person is a person other than he or such person ***(Section 416 of IPC)***
  - ***Section 66 D of IT Act deals with offence of impersonation using electronic means.e.ga*** person impersonating as bank manager and seeking private financial information through social engineering
- This is done to steal the personal information such as Date of Birth, Name, PAN number, Passport number, Credit card number, ATM Pin no., E-mail Account details, or any other unique identification feature etc and with an object to defraud. This sensitive information of the victim is obtained by various means like phishing, vishing sending the fake offers of rewards to the victim's email address and obtaining their confidential information.

CYBER STALKING

- Whoever follows / contacts any person or monitors his/her use of internet despite showing

clear sense of disinterest commits an offence of cyber stalking.Section 354(D) of IPC deals with stalking including cyber stalking.

- **Cyber Bullying :**-Causing harassment or creating fear through cyber stalking is cyber bullying.

  (Section 66E of IT Act deals with punishment for violation of privacy through computer network/computer resource)

- In this offence, by the use of computer or electronic devices, the victim is persistently followed, harassed and is threatened or intimidated by sending emails or by sending messages or calls on the mobile and by sending objectionable messages containing threat to the victim's Social Network Account causing mental and physical harm.

DATA THEFT

(Under Section 66 of the Information Technology Act, 2000 and under Section 379 of the Indian Penal Code, 1860)

- This offence involves unauthorized access and downloads, copies or extracts data from victim's computer containing sensitive information without the permission of the owner. This sensitive information includes the victim's personal information such as name, date of birth, address, contact details, username and password, credit card / debit card number OTP etc.

PORNOGRAPHY

- **Child Pornography :** Use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity. ***(Section 67 B of IT Act deals with Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form*** and under Section 292 of the Indian Penal Code, 1860 and Section 14 and 15 of POCSO Act)

- **Pornography :-** Transmission of obscene article/sexually explicit act/images through electronic means .

  (Section 67 and 67A of IT Act deals with punishment for transmission of obscene/ sexually explicit materials through electronic means)

- **Cyber Trafficking:** It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons.
- Publication of pornographic video, images, etc. through E-mail, website, chatting site, social network site etc. comes under the purview of obscenity crime
- The possession of above mentioned materials involving a child below the age of 18 years is itself an offence under Section 14 and 15 of the POCSO Act.

THEFT OF INTELLECTUAL PROPERTY AND TRADE SECRETS

(Under Section 66 of the Informational Technology Act, 2000; Intellectual Property Rights Act 1957 and Section 379 IPC and other enactments)

- This offence involves theft of intellectual property, business models, ideas, novelty and copyright protected works of an individual and organization by means of computer.

ESPIONAGE

(Under Sections 66 and 70 of the Information Technology Act, 2000)

- It involves gathering classified informations from the protected system of the governmental agencies . Through this, an attempt is made to get access to the sensitive governmental data.

HACKING

(Under Section 66 of Information Technology Act, 2000)

Hacking is a criminal offence committed by illegal use and control of a computer without the permission of the computer owner.

DENIAL OF SERVICE

Denial of Service attack:

- A DOS attack is disrupting the use of machine or network by its legitimate user by flooding it with superfluous traffic/requests .
- A DDOS (distributed denial of services attack is attacking the target system from multiple sources i.e using more than one unique IP Address making it difficult to trackthe source of attack.

(Under Section 66 of Information Technology Act, 2000)

This is a financial offence where access to computer or internet or both is obstructed for demand of money. Example: Salami attack, Ransomware etc.

❋ VIRUS OR WORM ATTACK

(Under Section 66 of Information Technology Act, 2000)

A program called virus that has the ability to infect other programs of the computer and make its copies and spread to other programs or computer. These are malicious software which attaches itself to any other software or they harm the computer. Use of such virus or worm to attack any computer device shall attract Section 66 of the IT Act and relevant provisions of the IPC.

❋ SPOOFING

(Under Section 66 & 66D of Information Technology Act, 2000)

Sending email by camouflaging it in a such a manner that it appears to have been sent from someone else's account to a victim demanding personal information etc.

SKIMMING

(Under Section 66C of Information Technology Act, 2000)

Obtaining card information by attaching unauthorized device to the ATM, POS machine etc. It is used against the victims to cause financial harm to them.

PHARMING

(Under Section 66 C & 66 D of Information Technology Act, 2000)

Pharming is that cyber crime where victim's private informations are deceptively extracted through a website which seems to be real and genuine, causing financial loss, where a malicious code is able to alter the host file on the target system .Once it is manipulated, all the traffic of the victim's system is misdirected to fake or fraudulent websites.

- **Crime against Government:-**
  - ***Cyber espionage*** – It is gaining illicit access to the confidential information/ data held by Government using computer network/resources.
  - ***Cyber Terrorism:-*** It is a politically motivated crime using computer resource/ computer network to cause serious disruption in services, bodily harm or injury to persons at large in order to create a sense of fear in the society so as to impinge upon the sovereignty, integrity and security of the State

Penalty for offences of cyber terrorism is dealt under sections of IPC, UAPA and the other applicable law along with 66 F of the IT Act

- Cyber warfare :- Cyber warfare is crime against Nations/Governments which may also include Cyber vandalism i.e. destroying/gaining access/modifying critical data stored in Government installations detrimental to the security of the State.

Description 2

JURISDICTION OF POLICE STATION IN REGISTERING FIR RELATED TO CYBERCRIME:

1. The concerned police station under the jurisdiction of which the Bank is situated from where there is illegal withdrawal of money will have the jurisdiction to register FIR under section 156 (1) read with section 177 of the Code of Procedure and investigate.

2. In cases of economic offenses where it is not certain under which jurisdiction the crime has been committed or if the crime has been committed under more than one jurisdiction or is a continuous offence, FIR can be registered in any related police station and investigation can be conducted under the provisions of Section 178 read with section 156 (1) Code of Criminal Procedure.

   Example - Money is withdrawn from the account of a person who is located in Ranchi by a criminal sitting in Jamtara and it is transferred to more than one account. There will be jurisdiction in all the places from where money has been transacted.

3. In cases where the offense has been committed within the jurisdiction of one police station and its effect will be in the jurisdiction of any other police station then the offence can be registered in either of the two police stations under the provisions of Section 156 (1) read with Section 189 of Code of Criminal Procedure.

   Example- In offences related to social media, if the objectionable post has been made within the jurisdiction of a police station, and it is uploaded on the social media through the Internet, and it is seen in other jurisdictions all the concerned police stations will have jurisdiction.

4. In case the offence is the result of a criminal conspiracy, both the police station will have jurisdiction to register FIR and investigate, where either the conspiracy was hatched or where the offence was committed, under the provisions of Section 180 read with Section 156(1) Code of Criminal Procedure.

   Example - In cases where the illegal withdrawal of funds through cyber crime has been done on more than one victim, and that amount has been transferred to a bank account in some other jurisdiction and the beneficiary is found accomplice under S. 120B IPC, then in this case the offence can be registered either in the jurisdiction of the bank account of the victim or the beneficiary and the investigation can be conducted.

5. In cases where financial offence or social media offence is done through telecommunication like internet, mobile etc., the place where the communication was made, or where it was received, both the police stations will have jurisdiction

under the provisions of Section 182 read with Section 156(1) of the Code of Criminal Procedure.

Example: If the OTP of an account holder is obtained by criminals sitting in the jurisdiction of any other police station through mobile or telecom and internet, then both the police stations will have jurisdiction.

STEPS TO BE TAKEN BY THE INVESTIGATING OFFICER AFTER THE REGISTRATION OF FIR RELATED TO THE CYBER CRIME:

1. To inform the concerned bank to block the account of the victim to avoid further withdrawals from the concerned account of the victim

   1) by phone

   2) by Internet, or,

   3) by personally visiting the concerned branch.

   The victim may however continue withdrawals /transaction from his account through checks or withdrawal slips.

2. To obtain details of the accounts from which illegal/unauthorized withdrawals have been made and the accounts in which funds have been transferred. A detailed transaction statement of the victim's bank account of the date of fraud should be obtained to track the channels through which the money has been routed. If the money has been transferred to a particular bank account through digital wallet/wallets ,a notice u/s 91 and 102 CrPC should be served to the concerned nodal officer to provide the information like transaction details ,associated IP Addresses and KYC of the concerned accounts and put a debit freeze on the accounts involved .A request should also be made for the reversal of fund to the source account after explaining the chain of transaction .A copy of the FIR and victim's bank statement should be attached in the email .

3. Similarly, to obtain details of the mobile or IP address such as CDR, CAF etc. using which crime has been committed from the internet service provider.

4. In this regard the following actions are required by I. O.-

To obtain copy of the statement of account duly certified under Section u/s 2A and 4 of the Bankers Book Evidence Act, 1891 from the branch manager of the concerned bank and section 65B of Indian Evidence Act (if a printout of the statement is taken)should be obtained from the beneficiary bank.

A notice u/s 91 CrPC should be served to the concerned ISP /TSP for providing the CDR and CAF of the mobile number in case of vishing frauds.

A certificate u/s 65B of Indian Evidence Act to be obtained from the concerned ISP

5. In case the above details are not supplied application may be filed in the concerned court having competent jurisdiction to issue notice under Section 91 of the Code of Criminal Procedure calling for the above documents.

6. In such cases where the above-mentioned details are not made available to the I.O. in due time after issuance of notice under Section 91 Cr.P.C the concerned court, if found appropriate, can take cognizance against the branch manager under Section 175 of the Indian Penal Code, 1860 by filing a separate case.

Or

The I.O. in such cases can also file a complaint under Section 195(1) (a) of the Code of Criminal Procedure, 1973 and make prayer to the court to take cognizance under Section 175 of the Indian Penal Code, 1860.

7. Where the account statement is received without certification the prescribed certificate under the provisions of Section 4 of Bankers Book Evidence Act, 1891 may also be obtained and presented to the court during the trial.

8. From which officer of the bank the statement of account may be obtained after due certification?

The Bank Managers or the Chief Accountant of every branch of the bank are competent to issue certified copies of book of accounts under the provisions of Section 2(8) of the Bankers Book Evidence Act, 1891.

9. In the light of the Section 4 of the Bankers Book Evidence Act, 1891 the certified copies of the book of accounts shall be admissible in the court of law as evidence and the bank officer issuing the same will not be required to be present in the court as a witness. In such circumstances where the statement of account is obtained by computer printout it will also be mandatory to take a certificate separately under the provisions of Section 65B (4) the Indian Evidence Act, 1872.

10. The certificate under Section 65B (4) of the Evidence Act, 1872 must be obtained from the service provider in case of CDR and other related electronic evidence and be filed in the Court and the above prescribed procedure of Section 91 Criminal Procedure Code, 1973 may be followed to obtain the said certificate.

11. The officer issuing the certificate under Section 65B (4) of the Evidence Act, 1872 **will not be required to be presented as a witness.** The said certificate will be **proved** by identification of the Investigating officer as recipient of the said certificate.

12. The certificate under Section 65B (4) Evidence Act, 1872 to be presented with the said CDR or electronic record as far as possible. But in the event of non-receipt of prescribed certificate during investigation it will be admissible by the court even during the trial.

13. The aforesaid procedure will also be followed to obtain CCTV footage. In order to identify the accused from CCTV footage his still photo obtained from the footage and after getting a certified photo of the accused from jail both can be sent to the expert for examination and report.

14. The prescribed certificates under Section 65B (4) of the Evidence Act, 1872 can be issued by putting digital signatures or signatures and seals under the provisions of Section 3 of I.T. Act

15. In illegal withdrawal cases where any other account is used for transfer and withdrawal of the amount which is not verified as per KYC rules of RBI, the bank officials opening the concerned account can also be charged under Section 120B of the Indian Penal Code, 1860 .

16. The persons who permit their bank account and ATM to be used in any manner for cyber crime can be charged under Section 413/411 along with other sections of the Indian Penal Code, 1860.

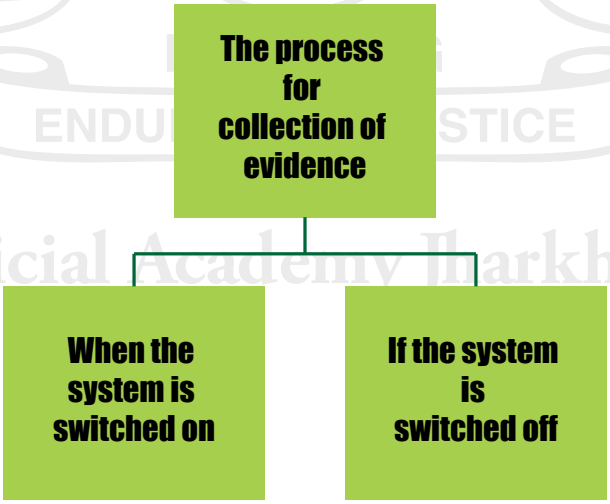
17. In cases where the victim or witness resides in any other police station area, there statement under the proviso I to section 161 Cr.P.C. may be recorded with the help of the Audio Video Electronic instrument to avoid undue delay. The investigating officer will mention the transcript of the said statement in case diary and he will also attach the audio and video of the said statement with the case diary.

❋ CRIME SCENE INVESTIGATION

Cyber crime scenes are totally different from traditional crimes. Electronic / Digital evidences are extremely fragile, they can easily be altered or tempered with. Therefore, utmost care must be taken in storage, examination and preservation of these evidences.

The steps to be followed at the place of occurrence:

- Proper identification and protection of the place of occurrence
- "As and where is" – a written description of the place of occurrence



- Forensic Duplication of electronic evidence and maintaining proper chain of custody of the electronic evidences and devices
- Recording statement of witnesses
- Classification of evidence

- Proper packaging and preservation of electronic evidence and electronic devices.

SEIZURE MEMO [PANCHNAMA] AND SEIZURE PROCEEDINGS

Section 165 of Criminal Procedure Code, 1973 and Section 30 of the Information Technology Act, 2000 authorizes the Investigating Officer for collection and seizure of evidences.

Seizure procedures are very important in cyber crime cases like any other crime. The Investigating officer is required to take extra precautions as per the nature of electronic / digital evidence. Basic knowledge of forensic tools and software along with competence in computer has great relevance in the context of proper search and seizure of electronic evidence.

THE FOLLOWING ARE THE NECESSARY GUIDELINES FOR THE PANCHNAMA:-

The seizure of electronic evidence to be made in terms of Section 100 of Cr.P.C. During seizure one technical expert who can correctly identify the equipment and give proper advice to the investigating officer should accompany him.

The time zone / system time plan plays a very important role in the entire Investigation process of electronic evidences. In the Panchnama, it should be ensured that the correct time is marked when the system is switch on mode along with its "hash value". If the system is found switched off, it should not be switched on.

It should be ensured that the serial number which is found on the system is also recorded in the Panchnama, so that the chain of custody is not broken.

Photographs of each device should be taken at the beginning of the Investigation at the place the device is found and if the hard disk is being detached from the device then its photograph must be taken.

CHAIN OF CUSTODY

The chain of custody provides written evidence regarding the delivery of electronic evidence as to when and to whom it is assigned. These are those people who seized the electronic device and who transfers the evidence from the place of occurrence, send it to the place of preservation, or to the forensic lab and then to the court.

THE MAIN POINTS IN THE CHAIN OF CUSTODY ARE:

- The storage medium or device should physically be inspected and photographed and must be preserved in a temper free environment after preparation of due seizure memo.
- Proper protection of evidence from theft and other disasters.
- Digital / electronic evidence must be protected from external electric and magnetic fields. Digital evidences especially compact discs must be protected from scratches and other physical damages.
- Minimum number of people should be involved in handling of digital evidences.
- Identification of electronic evidence and devices should be prominent, clear and written with permanent ink.
- The Investigating Officer should reach the place of occurrence with all the preparations for search and seizure . He should have proper and sufficient number of envelopes, bags and containers available for packaging of digital evidence.

DIGITAL EVIDENCE COLLECTION FORM (DEC)

Digital Evidence Collection is one important factor of cyber forensic which requires the evidence to be specific and completely accurate. The chain of custody should be properly documented and the electronic evidence in digital form be properly preserved.

The document to accompany the electronic evidence named 'Digital Evidence Collection Form'. The following details need enumeration in DEC Form -

- Crime Number
- Section of law involved
- Date - When the digital data or equipment is generated or sent to forensic lab for analysis.
- Name of the Investigating Officer
- Address - Location from where evidences were collected.
- Equipment related information
  - What type of equipment was seized such as - Hard Disk, Laptop, etc.

- Manufacturer – description of the manufacturer of the equipment
- Model No.
- Serial number of equipment
- Preserving hash value and maintaining chain of custody

THE INVESTIGATION NEED TO ADDRESS THE FOLLOWING QUESTIONS –

- When was the information regarding occurrence received by the victim / witness?
- Who can be the main suspect?
- How the occurrence took place?
- What damage is estimated?
- Is the offender a stranger?
- How will the cyber crime affect the victim?
- Which is the main system through which business is normally transacted
- What was done for identification, seizure, protection and analysis of concerned equipment/ device?
- Was the evidence collected by a specialist?

LEGAL PROCESS FOLLOWED AFTER THE DUE SEIZURE OF THE ELECTRONIC EVIDENCE

- The evidence collected in the course of Investigating, should be produced immediately before the court concerned.
- Orders of Court should be obtained for handing over digital evidence to expert for forensic analysis.
- In case the accused makes prayer for release of the seized articles, the Investigating officer must impress upon the court about the possibility of the electronic evidence being tempered with.

WHEN THE INVESTIGATING OFFICER FORWARDS THE COLLECTED ELECTRONIC EVIDENCE FOR FORENSIC ANALYSIS, THE FOLLOWING GUIDELINES SHOULD BE FOLLOWED.

The electronic evidence should accompany :

- Brief history of the case and the DEC form.
- The details of the exhibits seized and their place of seizure.
- The model, make and description of the hard disk or any storage medium
- The date and time of the visit to the place of occurrence.
- The condition of the computer system (on or off) at the place of occurrence.
- Is the photograph of the place of occurrence taken?
- Is it a stand-alone computer or in a network?
- Has the computer any internet connection or any networking with other computers?
- All electronic evidences must be examined by the examiner of electronic evidence notified under Section 79A IT Act 2000.
- All columns in the charge sheet must be filled carefully and the original documents and seized articles must accompany the charge sheet.

THE GUIDELINES FOR PREPARING THE CHARGE SHEET IN CYBER CRIME CASES :

- All the information shared by the complainant during registering the FIR / Course of investigation should be included in the Police Report.
- Make sure the section mention in FIR are still applicable and neither any of the sections have been repealed nor have been held unconstitutional. (Shreya Singhal v. Government of India, AIR 2015 SC 1523 wherein the Hon'ble Supreme Court has declared section 66A of Information Technology Amended Act as invalid).
- The documents proving the proper chain of custody of the electronic evidence must accompany the charge sheet.
- FSL report should be attached to the charge sheet.
- Please provide detailed information about the place of occurrence and the process the Investigating Officer has followed for digital analysis of electronic records.

Description 3

IN JHARKHAND THE FOLLOWING CYBER-CRIMES OCCUR MOST FREQUENTLY

1. Commission of fraud by making series calls on various mobile numbers and seeking the Debit/Credit card detail through various hacks of social engineering (Vishing Fraud)
2. Commission of financial fraud through spoof email
3. Vishing fraud using VoIP
4. ATM cloning by authenticating the Debit card details over IVR system of the banks
5. UPI (Unified Payment Interface)fraud by registering UPI on the registered mobile number of the victim after getting his details through social engineering
6. Financial frauds through E-commerce services like OLX by publishing fake sale offers using forged/impersonated identities

Illegal withdrawal of money from ATM

Posting of obscene and defamatory material on Social Network site / Cyber Stalking

Spoofing / Skimming

In case of the above crimes, the Investigating officer is expected to follow the following guidelines-

- The victim is supposed to lodge the FIR in the nearest police station pursuant to the order of the Hon'ble Supreme Court in the judgment of ***[Lalita Kumari v. State of Uttar Pradesh, (2014) 2 SCC 1]***
- Once FIR is registered, the Investigating officer can ask for the CAF, KYC of the victim's account and the beneficiary's account under Section 91 of Code of Criminal Procedure, 1973. The bank officer is required to provide all the information sought by the Investigating officer with the certificate mentioned under Section 65B(4) of Indian Evidence Act, 1872 within 24 hours without any delay (Section 167 Cr.P.C.).
- If the bank officer refuses or delay to provide these evidences without any reason, then legal action will be taken against the bank officer.
- The Investigating Officer will seek permission from the court to seize the bank accounts of the accused under section 102 of Criminal Procedure Code, 1973, the bank is under the obligation to seize those accounts in the compliance of Hon'ble

Supreme Court's Order ***[State of Maharashtra v. Tapas D. Neogy (1999) 7 SCC 685].***

- The victim can register the FIR for cyber stalking and posting of pornographic material on social network site in any police station under Section 354 (D) 1 (ii) of Indian Penal Code, 1860. If the police station in-charge refuses to register the FIR, then legal action will be taken against that police officer-in-charge. Registering of FIR is mandatory for the Police Station-in-Charge. ***[Lalita Kumari v. State of Uttar Pradesh, (2014) 2 SCC 1]***
- Where the printouts of offensive material is brought by the victim it shall be certified under section 65B of the Evidence Act by the victim and there is no need to further obtain certificate under section 65B (4) from the service provider and photographs submitted by the victim will be accepted as secondary evidence.

Note:-

- The Investigating officer will inform the victim about his right to file application for grant of compensation under Section 43A of the Information Technology Act 2000 before the Competent Authority (The Secretary of the Department of Information Technology of every State)
- The Investigating officer will also inform the victim about the circular of the Reserve Bank of India RBI/ 2017-18 /15 DBR.NO.Leg.BC.78 /09.07.005/ 2017-18 Dated 6/7/2017.

❑❑❑

Prepared by :

JUDICIAL ACADEMY JHARKHAND
Near Dhurwa Dam, Dhurwa, Ranchi-834004
Phone : 0651-2902833, 2902831, 2902834, Fax : 0651-2902834, 2902831
Email : judicialacademyjharkhand@yahoo.co.in
Website : www.jajharkhand.in

JHARKHAND STATE LEGAL SERVICES AUTHORITY
NYAYA SADAN, Near A.G. Office, Doranda, Ranchi
Phone : 0651-2481520, Fax : 0651-2482397
Email : jhalsaranchi@gmail.com
Website : www.jhalsa.org