SOCIAL ENGINEERING CRIMES

CYBER WARRIORS SERIES BOOK-3.0

सत्यमेव जयते

TELANGANA STATE POLICE

Duty
Honour
Compassion

TELANGANA STATE
POLICE

“Every Crime Tells its Tale,
Only it Needs
Someone to Read the Clues.”

SOCIAL ENGINEERING CRIMES

CYBER WARRIORS
SERIES
BOOK - 3.0

TELANGANA STATE POLICE

PREPARED BY:

1. K. Nagendar Rao
   Inspector, State IT Cell, Telangana

2. K. Srinath Reddy
   DSP, State IT Cell, Telangana

DESIGN & LAYOUT:

1. K. Venkataratnam (AAO)
2. Y. Ram Reddy
3. D.S.S. Prasad
4. B. Prakash
5. Y. Srinivas Rao
6. G. Shashikanth
7. T. Shashikanth

Special thanks to the following experts for their valuable suggestions and support in preparing this book.

1. **S.V. Ramana Murthy**
   Process Advisor, State IT Cell, Telangana
2. **M. H. Noble, Managing Director & his Cyber Forensic Team**
   Zoom Technologies India Pvt. Ltd.
3. **Anil Rachamalla**
   Founder, End Now Foundation
4. **KVM Prasad**
   ACP, Cyber Crime PS, Hyderabad Commissionerate
5. **S. Harinath**
   ACP, Cyber Crime PS, Rachakonda Commisisonerate
6. **K. Srinivas**
   Inspector, Cyber Crime PS, Cyberabad Commissionerate

FIRST EDITION: April *2022 (2000 Copies)*

PRINTED AT: DGP Press, Telangana State, Hyderabad

Disclaimer: The information contained herein has been obtained from several sources believed to be reliable. While compiling the contents of this book, care has been taken to provide the material lucidly. I would be happy to hear any suggestions, corrections, modifications, and topics to be addressed so that the same will be taken care of in the future.

DISTRIBUTION:
Restricted to Law Enforcement and Investigation Agencies

M. MAHENDAR REDDY, IPS.,
DIRECTOR GENERAL OF POLICE
Telangana State, Hyderabad.

Ph. Off : 040-23235170
040-23232831
Fax : 040-23296565
e-mail : dgp@tspolice.gov.in

MESSAGE

The advancements in digital communication technology and Internet services have been spreading at an amazing rate; they have also brought a paradigm shift in the lives of people. In no time, they became ubiquitous and part of people's lives. Their popularity has a dark side, as they provide new opportunities for those with criminal intentions and cybercrime activities as well. Nowadays, these cybercrime activities with social engineering techniques are evolving day after day. Further, Cybercriminals are becoming smarter and stronger in committing identity theft, online financial crimes, data theft, etc.

Social engineering crimes are increasing in intensity and number, and are causing emotional and financial damage to people. Social engineering techniques make cyber-attacks easier and help cyber criminals to avoid the arduous effort of locating and exploiting security vulnerabilities to access an individual's accounts or a network.

To respond to social engineering crimes efficiently and to provide help in the challenges faced while fighting against these threats, there is a great need for up-to-date information about social engineering techniques, novel investigation & detection techniques, and countermeasure techniques for police personnel. Thus, TS Police have brought out this book that illustrates an overview of Social Engineering Crimes and types of fraud - each covering specific topics relating to Modus Operandi, Expected Areas of Evidence, Standard Operating Procedures, Investigation & Detection techniques, etc. This has been followed by case studies of several cybercrimes & criminals.

I believe this book is sufficiently informative and extremely useful for all Police Officers to learn more about Social engineering threats, existing investigation & detection techniques, current measures, etc. It also provides necessary awareness to the staff of the Cybercrime vertical on Social Engineering Threats. Therefore, I recommend all Investigating Officers, and the Cyber Warriors working at all Police Stations, go through this book and acquire adequate knowledge in dealing with the menace of social engineering crimes.

I deeply appreciate and congratulate all the team members' dedicated efforts in bringing out this book.

29/4/22
(M.MAHENDAR REDDY, IPS)

FOREWORD

Prevention and detection of crime, both in physical space and cyberspace is a policeman's remit. Law Enforcement Organisations worldwide are grappling with the ever-increasing high volume, velocity, and variety of cybercrimes. While investigation officers, adept at handling traditional crimes may feel overwhelmed by this, a systematic approach would make most of these crimes solvable.

This book is an attempt by Telangana Police to create a Body of Knowledge for the officers working at the cutting edge level in preventing and detecting Cybercrimes. This effort by the state police headquarters is timely as it covers investigation techniques for new types of crimes that have been occurring in recent times.

This book is based on the experiences of some of our expert investigators and therefore written in a manner that users will find immensely practical. As criminals adopt new Modus Operandi and new techniques to unravel them develop, this book would need new avatars. For now, it eminently fills the void. Happy learning.

21/4/22

RAJESH KUMAR IPS,
Inspector General of Police
CI Cell, Intelligence Department,
Telangana, Hyderabad.

INTRODUCTION

The use of sophisticated technology and internet services is expected to increase significantly in the near future. Also, the community is expected to become involved in more sophisticated, targeted attacks. While syntactic attacks such as worms and viruses were previously spread to cause disruption and inconvenience, now the semantic social engineering methods are being used to steal personal information that may be used to infiltrate a network or system or to access an individual's financial accounts. Therefore, organised crime is expected to utilise this form of criminal activity and take a more active role in future high tech.

In today's digital world, social engineering attacks are the biggest threat. Social engineering is the process mainly aimed at tricking people into divulging private information that can be useful in cyber-attacks or providing them with sensitive data that are of use to an attacker. Cybercriminals use social engineering techniques to conceal their true identity and present themselves as trusted sources or individuals.

Although social engineering attacks differ from each other, they have a common pattern with similar phases. The common pattern involves the following four phases:

1) *Collect information about the target* - the attacker selects a victim based on some requirements.

2) *Develop a relationship with the target* - the attacker starts to gain the trust of the victim through direct contact or email communication.

3) *Exploit the available information and execute the attack* - the attacker influences the victim emotionally to provide sensitive information or perform security mistakes.

4) *Exit with no traces* - the attacker quits without leaving any proof.

There are many different types of social engineering attacks. Some forms of social engineering are convincing emails or text messages infected with links leading to malicious websites. Others involve more effort, like a phone call from a cybercriminal pretending to be a tech or customer care support requesting confidential information. Social engineering crimes are contemporary crimes that need to be addressed immediately. The characteristics like anonymity, borderlessness, and non-locality of cybercrime are posing severe problems for law enforcement. Further, the existing detection methods have fundamental limitations, and countermeasures are ineffective in coping with the ever-growing number of social engineering attacks.

Thus, there is a great need for more effective detection and countermeasure techniques to detect and minimise the impact of these attacks. In order to acquire skills to understand the social engineering trends and patterns, identify the areas of evidence, improve investigation methods, etc. - proper guidance is required for police officers. As such, this book is designed and prepared for the use of all Investigating Officers including Cyber Warriors working in Police Stations. This book also explains in-depth certain trends & patterns of social engineering crimes and management issues that arise. The narrative is constructed from a ground analysis of events and drawn upon a range of different sources about cybercrimes offending and victimisation.

1. SOCIAL ENGINEERING CRIMES

1.1 What is Social Engineering?

- Social engineering is the art of convincing people to compromise their computer/electronic systems. Rather than targeting equipment or software, fraudsters target humans who have access to information and manipulate their perceptions and make them divulge information using deception, influence, or persuasion.
- It's a known fact that hacking Human Mind is far easier than hacking a computer or business. Attackers go after human weaknesses like fear, greed, trust, desire, ego, sympathy, ignorance, carelessness, and haste.
- Social engineering attacks can include physical, social, and technical aspects employed in different stages of an attack. Fraudsters' attacking ways include email, instant messaging, phone, social networking, and websites.
- Fraudsters use many tools and techniques. These social engineering methods have few aspects in common. They all attempt to build rapport with victims by creating believable situations, establishing credibility, or creating a sense of urgency.
- Most of the time, people assume it's only the individuals who are prone to social engineering attacks and not the companies. No matter how big or low profile a business is, its employees will inevitably receive phishing messages giving scope to companies' information systems to be compromised.

1.2 Psychological Factors used by Fraudsters are:

- **Trust**: Exploiting that impulse is the basis of social engineering.
- **Ignorance**: Lack of knowledge about social engineering attacks makes people and organizations vulnerable.
- **Fear**: People are afraid of loss, and fraudsters exploit people's fears. For example, they might send a message or make a call warning about the possible loss of employment or money, or access.
- **Greed:** Fraudsters promise rewards in exchange for divulging information.
- **Moral duty**: People often feel obliged to help fraudsters when asked for help especially seeking donations during floods or Pandemic like Covid19.
- **Urgency**: A fraudster might call or email in the guise of a high-ranking chief executive officer who requires an urgent transfer of funds. They usually spoof emails posing as their boss.

- **Panic / Anger**: People don’t think clearly when pressured to act quickly. When Fraudsters call victims pretending to support and provide a frantic scenario that compromises safety.

1.3 Motivational Factor:

- **Financial Gain** – Many reasons can trigger motivation for financial gains, such as information gathering, organized crime, blackmail, etc.
- **Self-Education** – Few first-time hackers are motivated simply by the thrill of gaining knowledge and trying to beat the system for fun.
- **Revenge –** Unhappy/resigned employees could be doing it. They may even target an individual for not accepting a relationship.
- **External Pressure** – Blackmail, ransom, family pressure, and organized crime can be used to pressure an individual to commit a cybercrime.

1.4 Different Stages:

- **Information Gathering** – Internal phone directory; birth dates; organizational charts; personnel records, social activities, and relationships
- **Development of Relationship –** Psychological aspect of trust. The fraudster presents themselves as senior members of the organization to target to strengthen the relationship and trust.
- **The exploitation of Relationship** – Manipulation of the victim and obtaining the information like username and password and preparing to perform an illegal action
- **Execution to achieve the objective –** Having obtained the required personal/sensitive information, the fraudster can access the system and complete the illegal action.

1.5 Social Engineering Crimes – Methods:

- **Phone –** A fraudster calls up the victim and presents themselves as a person of authority, and uses techniques to extract the sensitive and personal information
- **Eavesdropping –** A fraudster may place themselves and secretly listen to a conversation overwork chat or in a lunchroom. Fraudsters gain access to the victim's computer system to obtain information that may later be used to commit cybercrime
- **Dumpster Diving –** Fraudsters gain access to the Company’s trash in an attempt to retrieve helpful documents, i.e., employee records organizational charts that may assist in a social engineering attack. They access old

computer equipment such as hard drives, unattended USB drives, and sticky notes on the unlocked screen.

- **Shoulder Surfing –** Overhearing on one's shoulder to see the password, PIN an employee is typing into the computer/ Mobile device.
- **Bogus Surveys –** False pop-up windows notify the individual that their internet connection has dropped out or simple survey form asking for feedback where they are required to enter their user details (username and password).
- **Phishing/ Vishing/ Smishing –** Hackers distribute emails/phones/SMS, presenting themselves to be from a legitimate organization (i.e., Bank or Govt. Organisation) and seek their personal and sensitive details to commit cybercrime.
- **Pharming –** Similar to phishing, users believe that they are entering their details (username, password) into a legitimate site. But, they are using a spoofed or mimicked site that emails the user's details to the hacker for future use.
- **Reverse Engineering –** Fraudsters execute a minor attack on the company to expose a vulnerability and then offer to "fix" the problem.
- **Baiting –** Baiting relies on the curiosity or greed of the victim. In this attack, attackers leave malware-infected USB flash drives in locations people will find them (bathrooms, elevators, sidewalks, parking lots, etc.), give their legitimate and curiosity-piquing labels, and wait for victims to use them.
- **Typo Squatting –** Fraudsters mimic the common brand URLs to gain trust. The fake website can easily collect information from victims if the typo is not noticed. e.g., www.bankofamerca.com instead of www.bankofamerica.com
- **Friendly Emails –** Fraudsters send an email either from a hacked friend's account or create a similar account using your friend's name. Often these emails have an attachment that contains malware.

2. FAKE CUSTOMER CARE FRAUD

Customer helpline number fraud is a common scam. It is a prevalent practice that we all reach out to the customer care numbers in Google or any search engine whenever we have any service-related issues such as payment transactions stuck or delays in shipment delivery. Fraudsters modify customer care details of a company on Google and push their fake number at the top of the search results. Thereby misdirecting the consumers into calling them.

There are two types of fraud, namely:

1. Fake Customer Care Number Present on Google and
2. Fake Tech Supports People calling to fix the problem/extend services.

In customer helpline number fraud, the fraudsters promote their number as being a legitimate helpline number for some business, service, or product. Victims who require a customer care number for any product or service usually search for such details on Google. When a customer calls, the scammer will try to elicit personal information such as Aadhar Number, PAN Number, bank account details, etc. In some cases, they might resort to a "man in the middle" attack where they get your information and log into the customer's account and do a transaction as a customer is doing it.

In the second case, i.e., Fake Tech-support fraud, fraudsters call the customer unexpectedly and inform them that they have detected a problem in the customer's computer and will help fix it. They then ask for access to the computer system and siphon the customer's data to use it for the wrong purposes. In some cases, they demand payment for the service provided.

The user must take a legitimate helpline/toll-free number from respective websites and apps. He has to see the support sections of the company for the correct contact numbers.

2.1 Modus Operandi:

When the user calls the fake toll-free/fake customer support numbers, they believe it to be a regular customer support center. Fraudsters mimic the official customer support centers' entire process, such as options, voice, and step-by-step processes.

Once the user calls the fake customer support, they start communicating and collect the victim’s complete details. Usually, they use social engineering techniques, where the fraudsters collect the Customer or target details, resulting in financial or personal data loss.

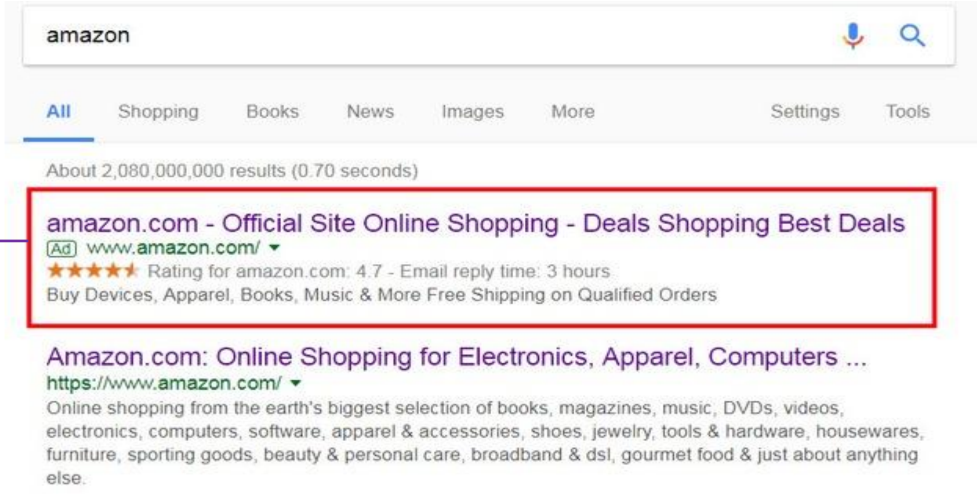
The fraudster also resorts to the following methods for collecting information from the customer:

a) They ask the customer to fill up a google form that asks for complete details and the OTP / PIN information.

b) Alternatively, they use screen sharing software (e.g., Any Desk, Team Viewer) to access the customer's screen and details such as OTP / PIN information, personal details, etc.

c) While in communication, the fraudster request customer to provide an acceptance or confirmation asking for OTP / PIN information.

d) If the victim realises that the money has been debited from his account and raises the question, the fraudster will request another transaction to refund the money. Again, he withdraws the money, and the process repeats.



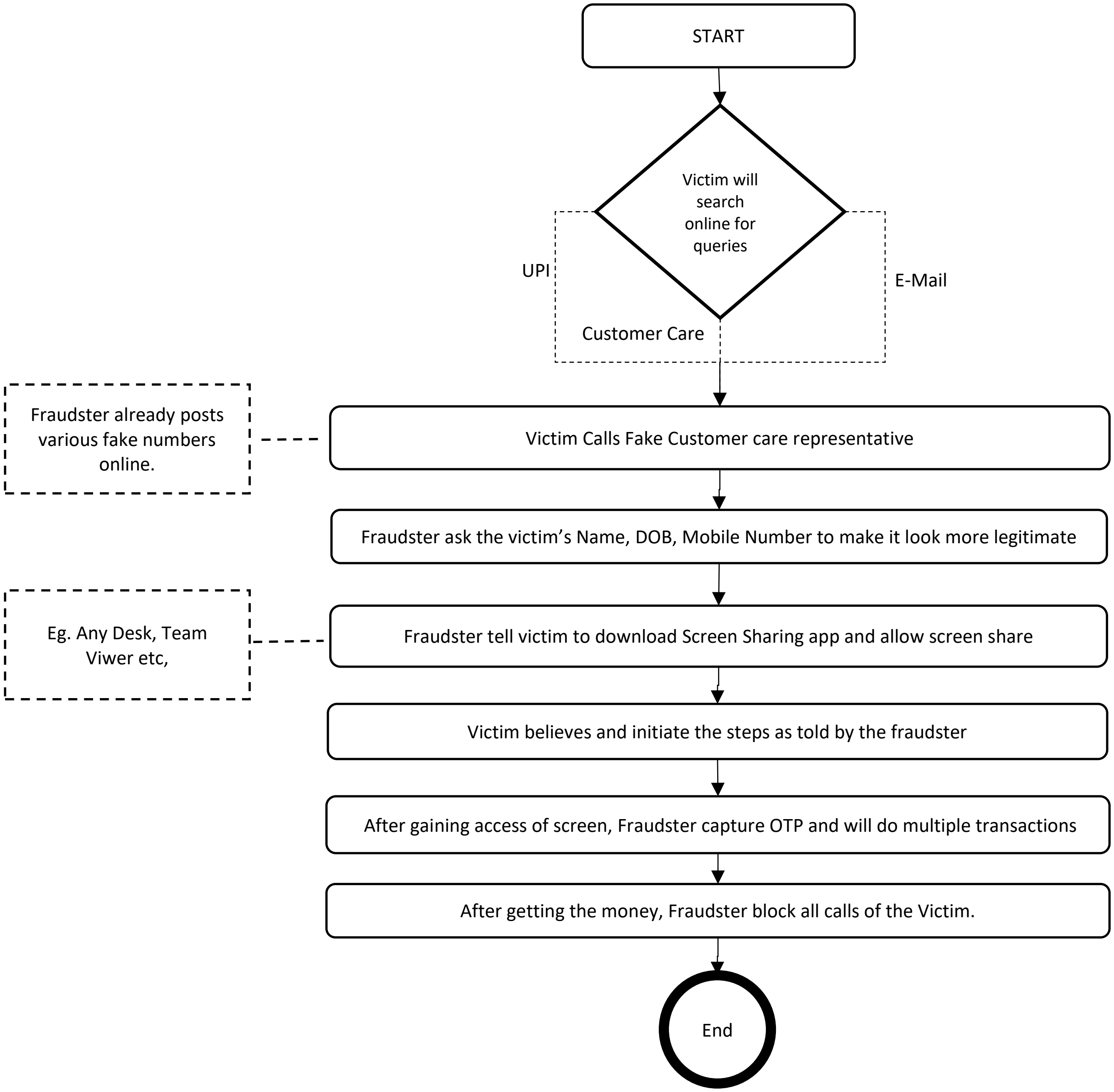
About 2,080,000,000 results (0.70 seconds)

amazon.com - Official Site Online Shopping - Deals Shopping Best Deals
Ad www.amazon.com/
★★★★★ Rating for amazon.com: 4.7 - Email reply time: 3 hours
Buy Devices, Apparel, Books, Music & More Free Shipping on Qualified Orders

Amazon.com: Online Shopping for Electronics, Apparel, Computers ...
https://www.amazon.com/
Online shopping from the earth's biggest selection of books, magazines, music, DVDs, videos, electronics, computers, software, apparel & accessories, shoes, jewelry, tools & hardware, housewares, furniture, sporting goods, beauty & personal care, broadband & dsl, gourmet food & just about anything else.

Be careful about **Ads** posted. This might not be the genuine website.

CUSTOMER CARE FRAUD - FLOW CHART


START
Victim will search online for queries
UPI
E-Mail
Customer Care
Fraudster already posts various fake numbers online.
Victim Calls Fake Customer care representative
Fraudster ask the victim's Name, DOB, Mobile Number to make it look more legitimate
Eg. Any Desk, Team Viwer etc,
Fraudster tell victim to download Screen Sharing app and allow screen share
Victim believes and initiate the steps as told by the fraudster
After gaining access of screen, Fraudster capture OTP and will do multiple transactions
After getting the money, Fraudster block all calls of the Victim.
End

2.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to safeguard the integrity of findings.

The IO can collect the following evidence for investigation purposes:

- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- Open the victim's account, collect screenshots of the fraud transactions
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroboration
- Last known location of the suspect/ accused
- The call recordings, if available on the mobile phone
- Screenshot of Google fake listing and links
- Find beneficiary accounts and funds transferred to multiple accounts.

2.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find the websites involved, find out the domain registrar from **whois.domaintools.com,** and address a notice u/sec 91 Cr. P.C requesting to furnish the registrant details, control Panel & I.P. logs, hosting details, and payment details.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- Send a request to the service provider to deactivate the accused’s mobile No so that the same number is not used for committing crimes.
- If the funds are transferred to wallets, notify U/Sec 91 Cr. P.C and collect registration details, wallet history, and transaction statement.
- Collect the CDR (Call Data Records) and CAF (Customer Application Form) of the suspect mobile numbers from which calls were received and linked to the bank account. From the CDRs, trace the suspect’s location and his contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.

- Search the suspect mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp Display image, Facebook account if available), True caller (for identifying name and suspect image if available) applications.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- Trace the accused by linking the series of events

2.4 Case Study:

Nature of Offence: Fake Customer Care

Case Details: The complainant received an SMS that Airtel Network service will expire within 24 hours, and a contact number (98327XXXX) is mentioned in that SMS for enquiry. A few minutes later, the complainant received a call from the above mobile number. The caller introduced himself as Airtel Customer Care Executive and requested to download the TEAMVIEWER QUICK SUPPORT App to update network service. Believing him as a genuine person, the complainant has downloaded an app on his mobile phone. As per the caller's instructions, he shared user-ID's user ID with the caller and allowed remote access notifications on that app. Later caller asked him to transfer Rs.10/- citing as processing charges. The complainant has transferred Rs.10/- using SBI Account as per the caller's directions. Immediately, the complainant started receiving SMSs that a total amount of Rs.2,40,000/- had been debited from the complainant's bank account in (05) transactions without his knowledge.

In this case, IO:

1) Sent Notices U/s 91 Cr. P.C to SBI Bank, Razor Pay, Novo Pay, Bharat Bill Pay with a request to furnish the beneficiary details of the fraudulent transactions
2) Addressed a requisition letter to Telecom Service Providers to furnish the SDR, CDR, and CAF of the accused / Suspects Mobile no.
3) Collected the bank statements of the fraudster and other related documents and obtained the beneficiary account details from concerned banks.
4) The Merchant's details, i.e., Bharath bill pay, Novopay, Roger Pay, and CDRs, revealed that the funds were transferred multiple times to different bank accounts.
5) Sent material objects to FSL for an Expert’s opinion

The main challenges, in this case, including getting the information about the persons who posted fake customer care numbers on the Internet (Google), addresses of the account holders provided by banks are found to be fake. Further, the account holders are spread across different states, making the investigation difficult.

3. UPI/OTP FRAUDS

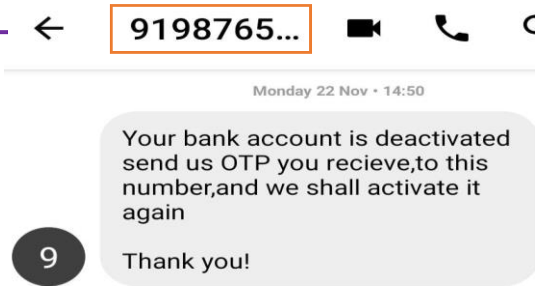
One of the Cybercrimes seeing a rise in recent times is Unified Payment Interface (UPI) fraud. It is a fast procedure to make digital transactions that facilitate cash payments swiftly, gaining more acceptance. Digital transactions have made life easy and, more importantly, time-saving. Now, the entire country is moving towards a cashless mode of payments. Various types of frauds take place on the UPI platform.

UPI is one of the most acceptable methods of payment during present times. We need a 4-digit PIN to authorize the financial transaction, and the entire transfer process is done in seconds. Of course, convenience comes with its share of liabilities. As the ease of online transactions progressed, the number of frauds in digital transactions surged to a new high. Fraudsters are using innovative methods to trick people.

3.1 Modus Operandi:

To capture the attention of targets/victims, fraudsters impersonate as bank staff and call for routine issues such as KYC updates, the redemption of bonus points, and cash backs.

- To make the call appear natural, they imitate the actual bank process by asking you to verify your date of birth, name, and mobile number, among other things.
- Fraudsters fabricate a tale so that the victim provides personal information to them to address the issue.
- The fraudster asks the victim to download screen sharing application to their phone. Such as TeamViewer and AnyDesk are available on the Play Store / App Store.
- The fraudsters request a one-time password (OTP) from the victim received on their phone.
- Once the screen-sharing app acquires all permissions required, the caller starts to take complete control of the victim's phone without their knowledge. After gaining full access to the phone, the fraudster grabs passwords and begins transacting with the victim's UPI account.



9198765...

Monday 22 Nov • 14:50

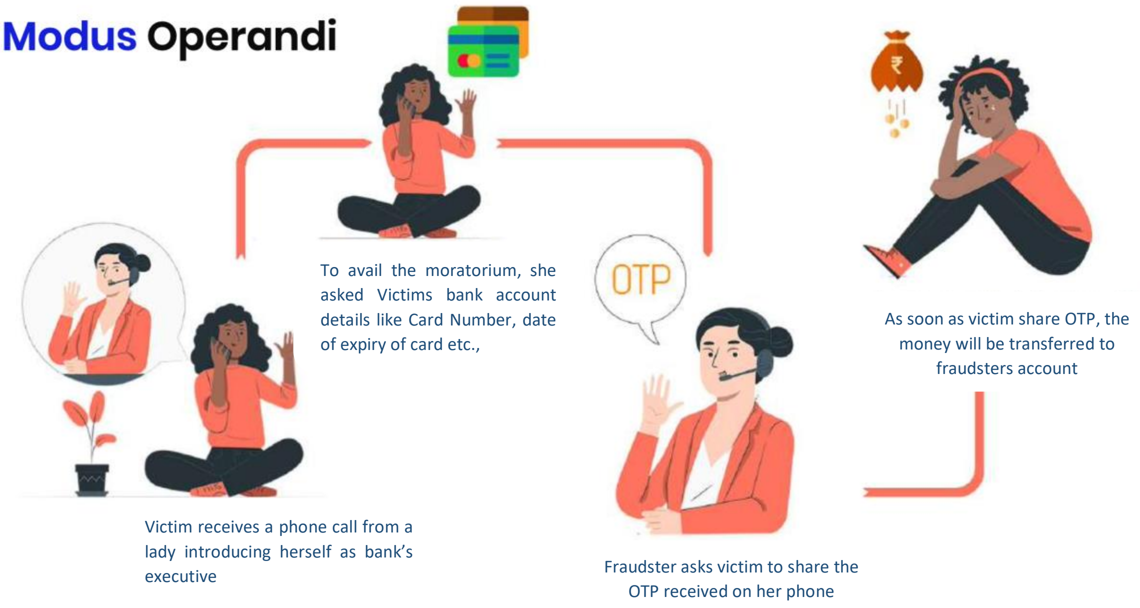
Your bank account is deactivated send us OTP you recieve,to this number,and we shall activate it again

Thank you!

FRAUD: OTP request from fraudster

Another method to commit OTP fraud:

- The Customer is asked to fill out the login, password, and OTP/UPI data via an SMS with short links and Google Forms.
- Alternatively, a fraudster (impersonat as a buyer) sends a payment request to the customer’s Virtual Payment Address on applications like Google Pay, PhonePe, Paytm, etc.
- Fraudsters (impersonating a buyer) send a Quick Response (QR) Code payment request to the customer's Virtual Payment Address.



Modus Operandi

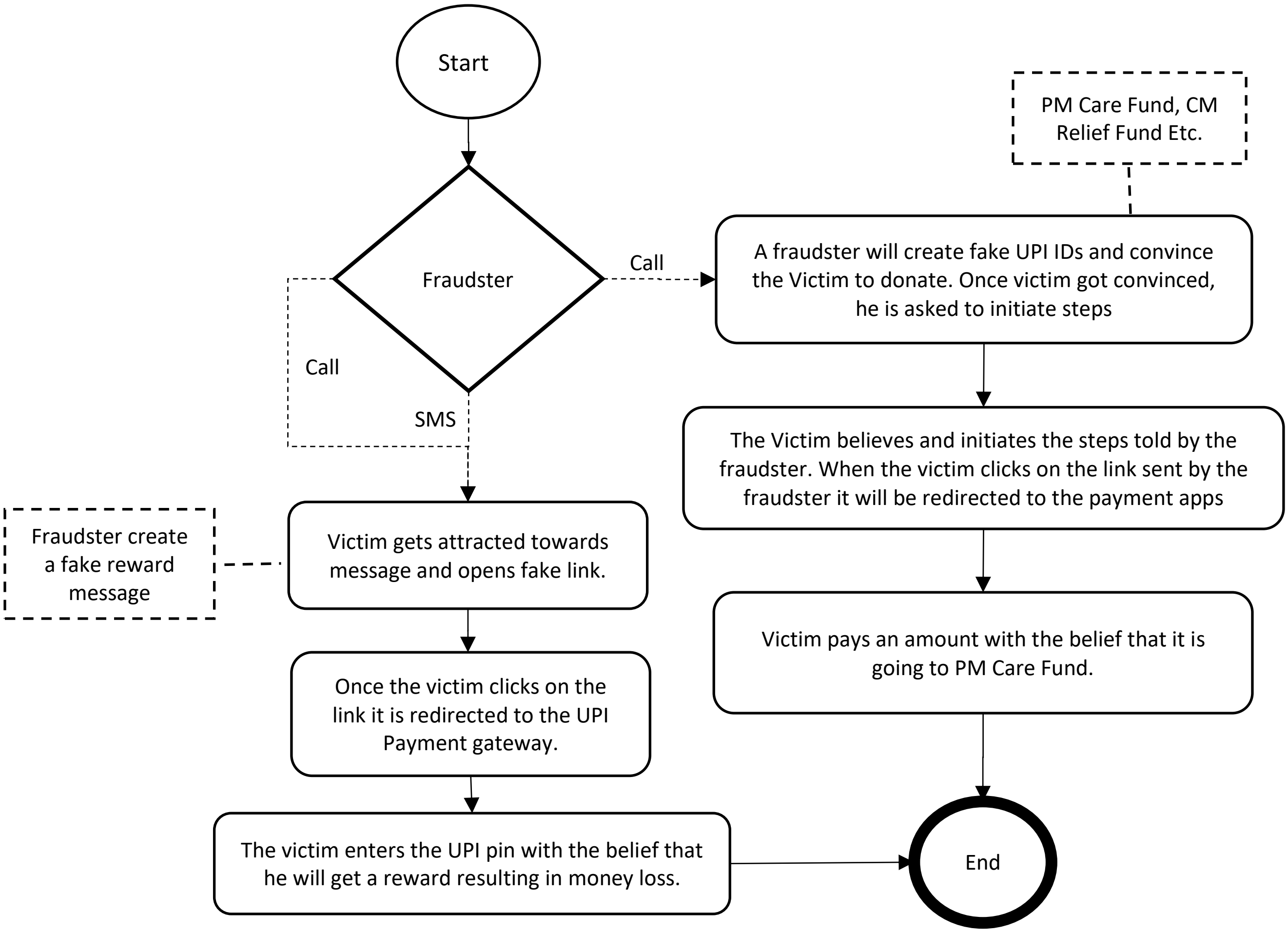
Victim receives a phone call from a lady introducing herself as bank’s executive

To avail the moratorium, she asked Victims bank account details like Card Number, date of expiry of card etc.,

Fraudster asks victim to share the OTP received on her phone

As soon as victim share OTP, the money will be transferred to fraudsters account

UPI Fraud - Flow Chart


Start
Fraudster
Call
Call
SMS
PM Care Fund, CM Relief Fund Etc.
A fraudster will create fake UPI IDs and convince the Victim to donate. Once victim got convinced, he is asked to initiate steps
The Victim believes and initiates the steps told by the fraudster. When the victim clicks on the link sent by the fraudster it will be redirected to the payment apps
Victim pays an amount with the belief that it is going to PM Care Fund.
Fraudster create a fake reward message
Victim gets attracted towards message and opens fake link.
Once the victim clicks on the link it is redirected to the UPI Payment gateway.
The victim enters the UPI pin with the belief that he will get a reward resulting in money loss.
End

3.2 Expected Areas of Evidence:

Once the FIR is registered, the investigating officer needs to start with given inputs from the victim and contact Bank/Financial institution to get the required information to trace the location of the fraudster.

The IO can collect the following evidence and other information for investigation purposes:

- The bank account and credit card data used for transactions.
- The screenshots of specific fraud UPI Transaction Details
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)

- Open the victim's account, collect screenshots of the fraud transactions
- Details of Beneficiary account and funds transferred to multiple accounts
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroborations.
- The call recordings, if available on the mobile phone
- The victim's registered mobile number, email address, PAN, ATM card number(s), and other proofs linked to the account.
- Details of Login/Logout IPs of the transactions
- IP Address of the device where the actual fund is transferred
- In case of money withdrawals, CCTV footage of ATM Centre for a particular duration
- Details of money Withdrawals locations
- Check the mobile service provided on the address and identity proofs
- Any other relevant information deemed fit for the investigation.

3.3 Standard Operating Procedure (SOP):

One-time Password (OTP) Fraud:

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find out from which phone number the victim has received the OTP.
- Search the suspected mobile numbers in open-source tools such as Eyecon & Truecaller (for identifying name and suspect image if available) applications.
- Send a request to the service provider to deactivate the accused’s phone number so that the same number is not used for committing crimes
- Collect a copy of the bank account statement from the victim.
- Serve a notice U/sec 91 Cr. P.C to the nodal team and collect the details like the phone number of the accused, from which they communicated to the victim, and identify the service provider that suspect is using.
- Ask the victim to change their credentials for bank accounts.
- Collect the information of the mobile number and its service provider Ex: Airtel, Reliance JIO, BSNL, etc.,
- Request service provider for SDR, CDR, IPDR, and IMEI for further analysis.
- Trace the suspect locations and filter the location by eliminating the mobile numbers that are genuine and long-term users.
- Request for freezing of the account
- Trace the accused by linking the series of events

Unified Payment Interface (UPI) Fraud

- Find out from which phone number the victim has received the QR code.
- Also, check the victim's bank statement and determine when and how the withdrawals took place.
- Identify to which suspect account the money has been transferred.
- If any other services availed are found, serve notice u/sec 91 Cr. P.C and collect the registration details, mobile numbers, email IDs, etc.
- Ask the victim to change their credentials for bank accounts
- Ask the victim to change the UPI pin code for security purposes.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts.
- Request for freezing of the fraudster/ beneficiary account
- Link the series of events to trace the accused.

3.4 Case Study

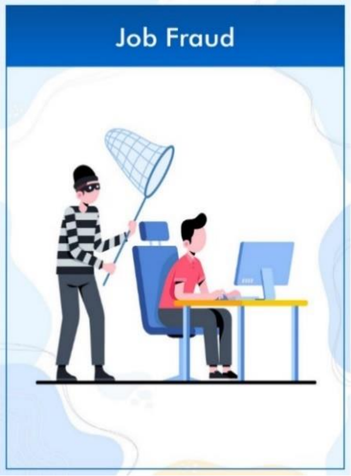
Nature of Offence: UPI/OTP Fraud

Case Details: The complainant received a call from an unknown number (89549xxxxx) and introduced his profession as an SBI agent from SBI Credit card Department with his ID No: SBIN00XX. And he told the complainant that he would increase the complainant’s Credit card limit. He asked to share the complainant's Credit card details like Card Number, CVV, and OTP. So the complaint believed it to be a genuine call and disclosed all the credentials as asked. The complainant was asked to share other Credit card details to increase its limit. Again, the complainant believed and revealed the Axis Credit card credentials like No: 53056205XXXXX, CVV, and OTP. Immediately the fraudster debited the amount from his both Credit cards in two (02) transactions Rs.90, 000/- and Rs.50,000/-

In this case, IO:

1. Sent Notices U/s 91 Cr. P.C to Paytm and the Credit Card department to furnish the beneficiary details of the fraudulent transactions and obtain the KYC and linked mobile numbers.
2. Addressed a requisition letter to Telecom Service Providers to furnish the CDRs of accused mobile numbers.
3. Identified the beneficiary details and address of the accused
4. Based on the evidence collected, the accused was arrested
5. The main challenge in the case investigation is that the accused furnished the fake address to the Bank, making the investigation difficult.
6. Sent material objects to FSL for an Expert’s opinion

4. JOB FRAUD



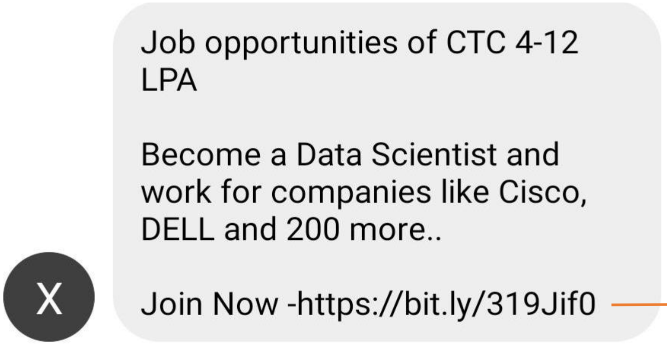
Cybercriminals target unemployed youth in the name of job offers. They advertise jobs in the same way legitimate employers do. In this type of fraud, fraudsters get data of unemployed youth from Job Portals, darknet then place ads in major newspapers, distribute pamphlets, send bulk mailers, and even call victims directly over the phone. Usually, criminals pose as company recruiting agents/officials. Criminals initially operate via telephone and e-mail. They book opulent hotels for interviews. They demand a security deposit and interview fee; they give a forged appointment letter and then vanish. They also maintain fake websites of reputable companies, employment marketplaces, and government departments to deceive candidates. E-mails are sent with official-looking documents asking either for private information or early payment.

Types of frauds:

- **Background Entry Job fraud–** Skipping all formal interview processes and getting a job without being qualified officially in reputed organizations.
- **Work from Home Job Fraud** - Offered to be employed at home for doing very simple tasks with minimal effort for a considerable income.
- **Social Media Following Fraud**- The victim is lured by an offer for doing some simple task (Follow, Like, Share, and Comment) in exchange for a hefty income.
- **Abroad Job / Education Fraud** - Offers a visa guarantee for a Job / Education for a hefty charge.
- **Career Consulting Fraud** – Offers resume writing, resume forwarding, organizing interviews, or other career-related services for a charge.

4.1 Modus Operandi:

- Fraudsters get data of unemployed youth from Job Portals, the darknet, etc.
- Fraudsters advertise on social media, send mass emails, or approach new victims through a victim who has paid money (advances) for the job.
- Victims get lured with the emails, and then they complete the interview formalities. They are informed that they are selected and ask them to pay amounts (advances, referral fees, deposits, etc.)
- Once the amount is transferred, the victim doesn't get any response from the fraudsters.



Job opportunities of CTC 4-12 LPA

Become a Data Scientist and work for companies like Cisco, DELL and 200 more..

Join Now -https://bit.ly/319Jif0

High package and Beware of links.

Red flags:

a) Getting the job immediately after a quick phone or Instant Message interview.

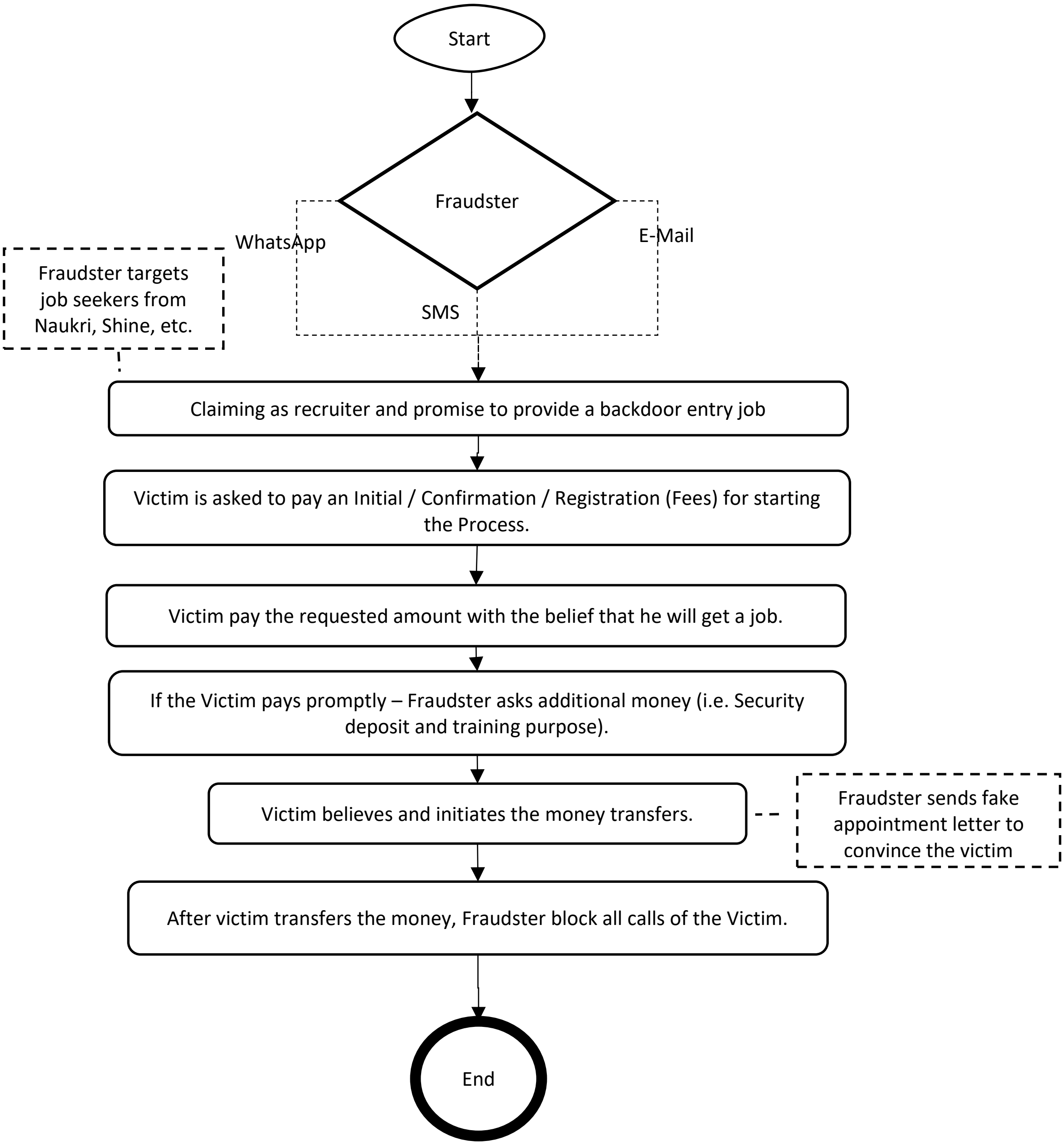
b) Many fraud Emails will look legitimate, but they are unprofessionally written, and here are some signs to detect fraud emails.

- Sending mails from Gmail / Yahoo Accounts instead of their official domain emails
- Alternatively, they might use a spoofed website, i.e., jobs@bankof_america.com instead of jobs@bankofamerica.com
- No Salutation, i.e., Mr. or Ms., means a template is compiled and pasted for many people.
- Capitalization errors: hyderabad, it should be Hyderabad.
- Punctuation, Commas, Periods, Paragraph, and Full of Grammatical errors
- Email Signatures have only mobile numbers, and they do not publish an official number with an extension.
- Email ID may be spoofed; Please check the Email header thoroughly

c) Google/ LinkedIn / Official Domain search results do not show accurate results of the openings interviewed.

d) Fraudsters ask victims to Provide Private Information (Aadhar. PAN, and Passport copies) under the pretext of Background Checks to private mail IDs instead of the official ones.

Job Fraud - Flow Chart


Start
Fraudster
WhatsApp
E-Mail
SMS
Fraudster targets job seekers from Naukri, Shine, etc.
Claiming as recruiter and promise to provide a backdoor entry job
Victim is asked to pay an Initial / Confirmation / Registration (Fees) for starting the Process.
Victim pay the requested amount with the belief that he will get a job.
If the Victim pays promptly – Fraudster asks additional money (i.e. Security deposit and training purpose).
Victim believes and initiates the money transfers.
Fraudster sends fake appointment letter to convince the victim
After victim transfers the money, Fraudster block all calls of the Victim.
End

4.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to safeguard the integrity of evidence.

The IO can collect the following evidence for investigation purposes:

- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- The screenshots of specific UPI Transaction Details, if applicable
- Beneficiary account details and funds transferred to multiple accounts
- The Company name, Job titles used by the fraudsters
- Open the victim's account, collect screenshots of the fraud transactions
- The website link, email ID, and Mobile Number of the accused from the Victim
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroborations.
- The call recordings, if available on the mobile phone

4.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find out the suspect mail belongs to which email service provider. Ex: Gmail, Yahoo, Hotmail, etc. Serve a notice U/sec 91 Cr. P.C to the nodal team and collect the registration details, I.P. logs, registered mobile number, recovery mail ID, etc.
- Check the mail source or header to find whether mail is routed through the proper channel. If the mail ID is routed through a fake mail service, address a mail to the fake service provider and collect the original I.P. logs.
- After collecting the details from the mail service provider, identify the ISP (Internet service provider) and send a notice U/Sec 91 Cr. P.C to the concerned ISP to obtain the user details.
- If any website is used by the accused similar to genuine sites, find out the domain registrar from whois.domaintools.com and address them a notice u/sec 91 Cr. P.C requesting to furnish the registrant details, control Panel & I.P. logs, hosting details, and payment details.
- Analyze the victim's bank statement and find the beneficiary accounts.
- Collect SDR, CDR, IPDR, and IMEI for all suspect numbers for further analysis.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to

the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.

- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If amounts are transferred to e-wallets, serve notice U/sec 91 Cr. P.C to concerned e-wallets like Paytm, Phonepe, etc., and collect registration details, wallet history, and transaction statement.
- If the payment is made through any website/portal, find out the payment gateway and serve notice u/sec 91 Cr. P.C requesting registration details, linked bank account details of merchant/customer.
- Collect the CDRs and CAFs of the mobile numbers used to contact the complainant. From the CDRs, trace the suspect's locations his contacts. From the messages/alerts received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Request for freezing of the fraudster/ beneficiary account
- Send a request to the Sevice Provider to deactivate the Mobile Number of the accused so that the same number is not used for committing crimes
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- If any other services availed are found, serve notice u/sec 91 Cr. P.C and collect the registration details, mobile numbers, email IDs, etc.
- Trace the accused by linking the series of events

4.4 Case Study:

Nature of offence: Job Fraud

Case details: A complaint is received from 56 years old retired govt employee from Hyderabad stating that he lost Rs. 47,00,000/- (forty-seven lakhs rupees) in the name of getting a job in a foreign country. He stated that he received a phone call from an unknown person and introduced himself as CEO of a reputed company in California, America. He mentioned that the complainant got shortlisted for Chief Manager Role in his company and asked willingness to attend an interview held in New Delhi. Complainant given willingness to attend for that. The next day complainant received a phone call introducing himself as Customs Officer at New Delhi Airport, stating that Miss. Heather Williams landed at Delhi Airport & carried a DD of US $ 1,75,000; asked the complainant to pay Rs.55,000/- for the release of DD in provided account number, which was communicated in a fake mail ID. Further Miss. Heather Williams forced the complainant to deposit money of Rs. 10,00,000/-. Four days later, a fake customs officer asked for Rs.8,65,000/- in the call. After two days, a person introduced himself as Public Relations Officer British Consulate-New Delhi, contacted through Whatsapp and convinced Rs.1,23,97,500/- would be credited within a week if he pays the amounts asked by previous callers. One ATM Card was sent to the complainant, and the password was shared through mail ID. After checking the card, the complainant informed the fraudsters that the balance on that card was only Rs.9700/-. On that, fraudsters asked the complainant Rs.8,65,000/- to get credit money on that card, which he believed and paid. The amount of Rs.47,00,000/- (forty-seven lakhs) was deposited into fraudsters' accounts in 42 transactions of 11 different bank accounts in 98 days.

In this case, IO:

1. Collected phone numbers of fraudsters from the victim and sent notices U/Sec 91 Cr.P.C. to service providers
2. Identified the beneficiary account and obtained transaction details from the bank.
3. Identified the ATM Card details from the concerned bank
4. Collected CDR, CAF, SDR, and IMEI details of the accused's mobile number
5. Identified the residing location of the accused based on CDR analysis
6. Sent material objects to FSL for an Expert's opinion

5. KYC UPDATION FRAUD

Know Your Customer (KYC) is the mandatory process of verifying a client’s identity when opening an account and existing customers at periodic intervals. It is one of the common cyber frauds in India. Presently, the whole country is moving towards a cashless economy. UPI is a quick method to make payments digitally and is rapidly gaining popularity. Digital transactions have made life easier and saves time. Fraudsters have used KYC procedures with social engineering strategies to steal people's hard-earned money. They target persons who are unfamiliar with these technologies.

There are two types of KYC frauds, namely:

1. KYC frauds through SMS / Email / Phone
2. Refunds or Cash-Back or expiring reward points through SMS / Email / Phone

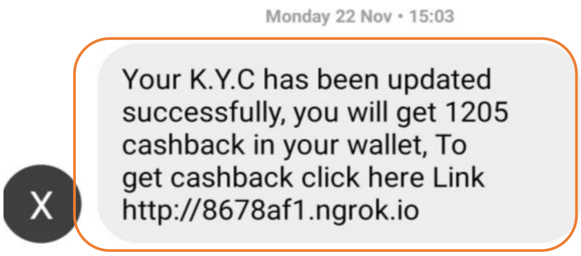
In the first case, the customer gets an SMS / Email having Short Links requesting to update the KYC of a Bank / Aadhar Card or a PAN Card. When the customer clicks the link and fills up the detail, the customer also fills in the OTP details. All details are automatically forwarded to the fraudster’s phone, who then transfers money using the OTP from the customer's account.

In the second case, i.e., fraudsters trick users with issues like refund or cash-back or expiry of credit card reward points, etc.

5.1 Modus Operandi:

a) Fraudsters impersonate as a bank representative to make the call sound legitimate, calling for routine issues such as KYC updates, bonus point redemption, and cash-backs. They mimic the actual bank process by asking verification questions about the personal information to make the call sound more professional.

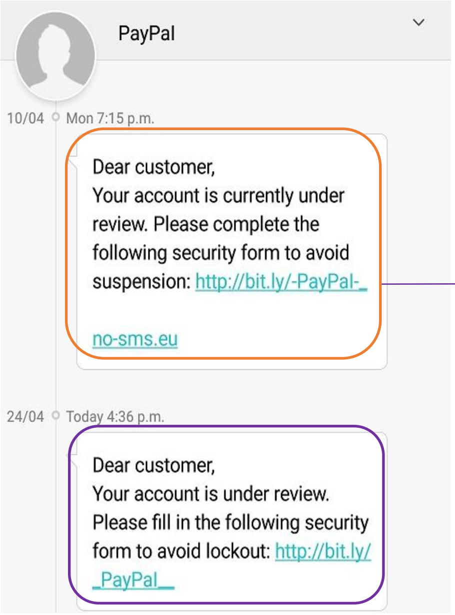
b) Fraudsters use social engineering tactics to fabricate a scenario where they force the victim to provide personal information to resolve the problem.



Monday 22 Nov • 15:03

Your K.Y.C has been updated successfully, you will get 1205 cashback in your wallet, To get cashback click here Link http://8678af1.ngrok.io

Be aware of NGROK link.



PayPal

10/04 Mon 7:15 p.m.

Dear customer,
Your account is currently under review. Please complete the following security form to avoid suspension: http://bit.ly/-PayPal-_

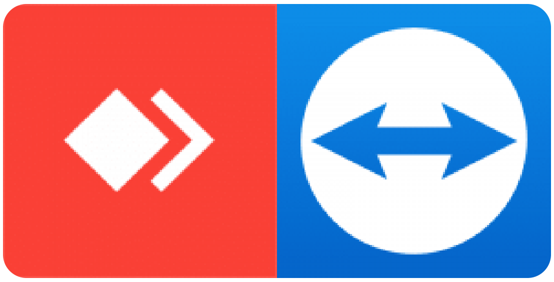
no-sms.eu

24/04 Today 4:36 p.m.

Dear customer,
Your account is under review. Please fill in the following security form to avoid lockout: http://bit.ly/_PayPal_

Never click on external links and update your information

They ask the victim to download screen-sharing applications on their phones, such as Any Desk, TeamViewer, and other screen-sharing apps available on the Play Store / App Store.

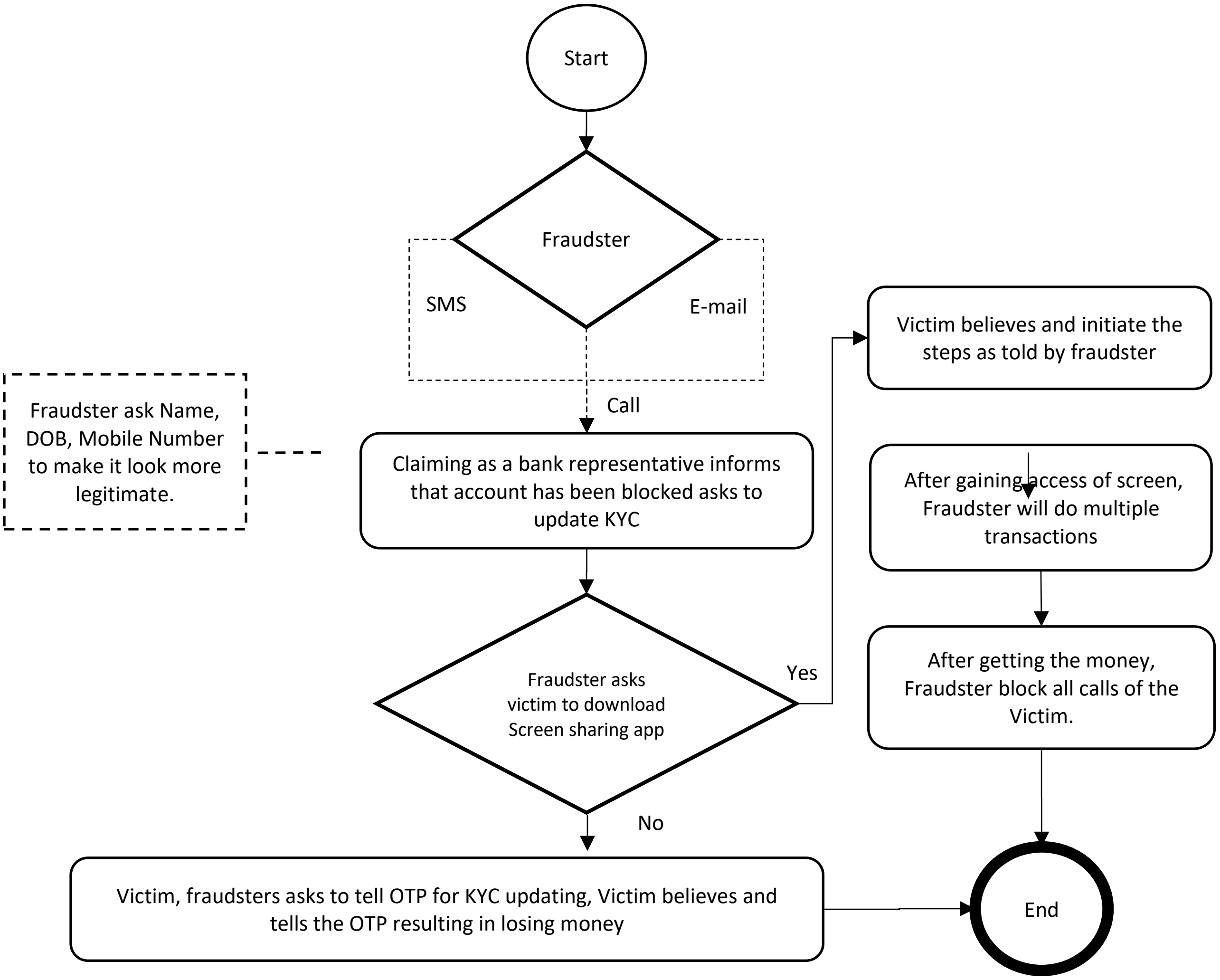


Any Desk TeamViewer

c) The fraudsters will then ask the person (victim) for an OTP that is received on their phone. After the victim shares OTP, the fraudster asks them to grant permission from the phone.

d) When the fraudster obtains all the necessary permissions, he takes complete control of the victim's phone without the victim's knowledge. After gaining full control of the phone, the fraudster recovers passwords and begins transacting with the victim's UPI account, causing financial loss.

KYC Fraud - Flow Chart


Start
Fraudster
SMS
E-mail
Call
Fraudster ask Name, DOB, Mobile Number to make it look more legitimate.
Claiming as a bank representative informs that account has been blocked asks to update KYC
Fraudster asks victim to download Screen sharing app
Yes
No
Victim believes and initiate the steps as told by fraudster
After gaining access of screen, Fraudster will do multiple transactions
After getting the money, Fraudster block all calls of the Victim.
Victim, fraudsters asks to tell OTP for KYC updating, Victim believes and tells the OTP resulting in losing money
End

5.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to maintain the integrity of evidence.

The IO can collect the following evidence for investigation purposes:

- The bank account and credit card data used for transactions.
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)

- The details of login/logout I.P address along with the date and time of fraudulent transaction
- The details of the beneficiary account
- The specific Location history
- The Geo-Location of the alleged user
- The details of linked Wallets and bank A/Cs of the culprit
- Details of the fraud transactions
- The call recordings, if available on the mobile phone
- Mobil Number, e-mail ID of accused

5.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- If the complainant received a message to update KYC, Collect the sender Bulk SMS Ex: QP-SBIKYC from the following link https://www.findandtrace.com/trace-bulk-sms-sender
- Identify the service provider and serve a notice U/sec 91 Cr. P.C to collect the user details, KYC documents, etc.
- Identify how the data is compromised by using remote access applications like Team Viewer, Quick Support, Any desk, etc.
- Identify recently installed applications, check if the victim installed any remote application, and if yes, serve notice U/Sec 91 Cr. P.C to the service provider and find the user details.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts.
- Send a request to the Service Provider to deactivate the Mobile Number of the accused so that the same number is not used for committing crimes.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If amounts are transferred to e-wallets, serve notice U/sec 91 Cr. P.C to concerned e-wallets like Paytm, Phonepe, etc., and collect registration details, wallet history, and transaction statements.
- Collect the CDRs & CAFs of the mobile numbers from which calls are received. From the CDRs, trace the suspect's locations his contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.

- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- If any other services availed are found, serve notice u/sec 91 Cr. P.C and collect the registration details, mobile numbers, email IDs, etc.
- Initiate the process of refunding of the amount to the victim.
- Trace the accused by linking the series of events

5.4 Case Study:

a) Nature of offence: KYC Fraud

The complainant received an SMS from XYZ bank that, as per GOI-Government of India regulation, he has to update his KYC as early as possible or his account is blocked, and the message also has a link. By clicking on the link provided, he can directly update his KYC details. Upon clicking the link, it asked for his details, such as his Aadhar card and bank card details. He was tricked into giving away his identity card and bank account details and got duped for 2 lakh rupees.

In this case, IO:

1. Identified the number from which SMS was received. The number was found to be a fake number freely available online for sending
2. Sent 91 Cr.P.C. notice to SMS Service provider for details
3. Identified the beneficiary account details to which Rs.2 Lakhs transferred
4. Collected bulk SMS IP records to identify the suspect/ accused location
5. Traced the accused based on analysis of SMS IP records
6. Sent material objects to FSL for an Expert's opinion

6. OLX FRAUDS

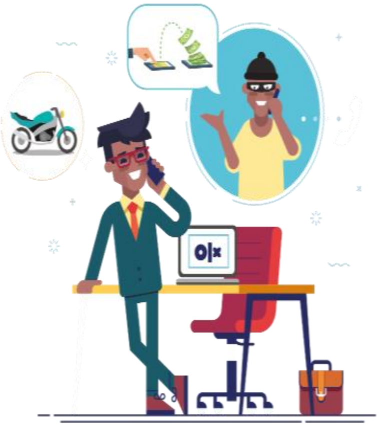
OLX is a leading platform to buy and sell goods and services. The public's lack of knowledge of app-based payment services and UPI helps fraudsters in making quick cash. In this type of fraud, the fraudster usually poses as an army/ paramilitary officer, contacts a person selling products on websites like OLX and Quikr, and readily agrees to pay the asked price.

It may be a surprise that well-educated netizens in metro cities are victims of "OLX Frauds." On this platform, either a buyer or a seller could be a target, and the majority of the people (victims) are first-time application users.

6.1 Modus Operandi:

Fraudster as a Buyer

Anyone can expect a call from a probable buyer as soon as an advertisement is posted on the portal,



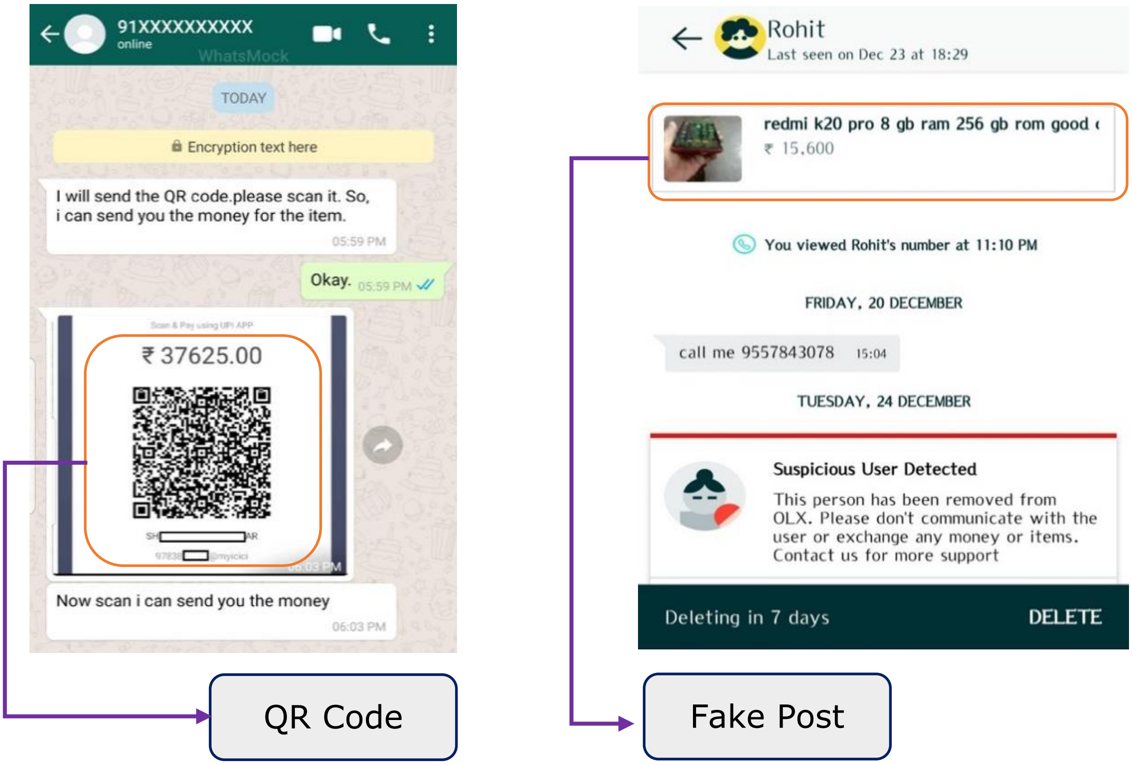
- The buyer (fraudster) would never bargain and will accept any price posted on the portal for the item.
- The caller would act as if he is trying to transfer money; he sends a QR Code to the seller to scan or UPI/OTP number to be sent as received by the seller.
- They use simple social engineering tricks, keep the victim in a continuous phone conversation and create panic by urging them to close the deal as early as possible; during the conversation, victims end up handing over OTP/UPI or scanning the QR code and lose their money instead of receiving the money
- After payments are made, the fraudster will block victims' numbers or switch off their phones.

Fraudster as a Seller

A fraudster attempts to contact the victim and sell something for less than one-fourth of the market price, which is a red flag.

- The fraudster is desperate to sell the merchandise, claiming to be a military officer.
- To symbolize acceptance, the caller will ask the victim to submit some advance money via UPI or QR Code.

- They use basic social engineering techniques to keep the victim on the phone and create panic by urging him to close the deal as soon as possible and requesting to send money for Military Transportation Charges, GST Charges, Inter State Taxes, etc.
- After receiving money, they block the victim's number or turn off their phones.



I will send the QR code.please scan it. So, i can send you the money for the item. 05:59 PM

Okay. 05:59 PM

Now scan i can send you the money 06:03 PM

redmi k20 pro 8 gb ram 256 gb rom good c
₹ 15,600

You viewed Rohit's number at 11:10 PM

FRIDAY, 20 DECEMBER

call me 9557843078 15:04

TUESDAY, 24 DECEMBER

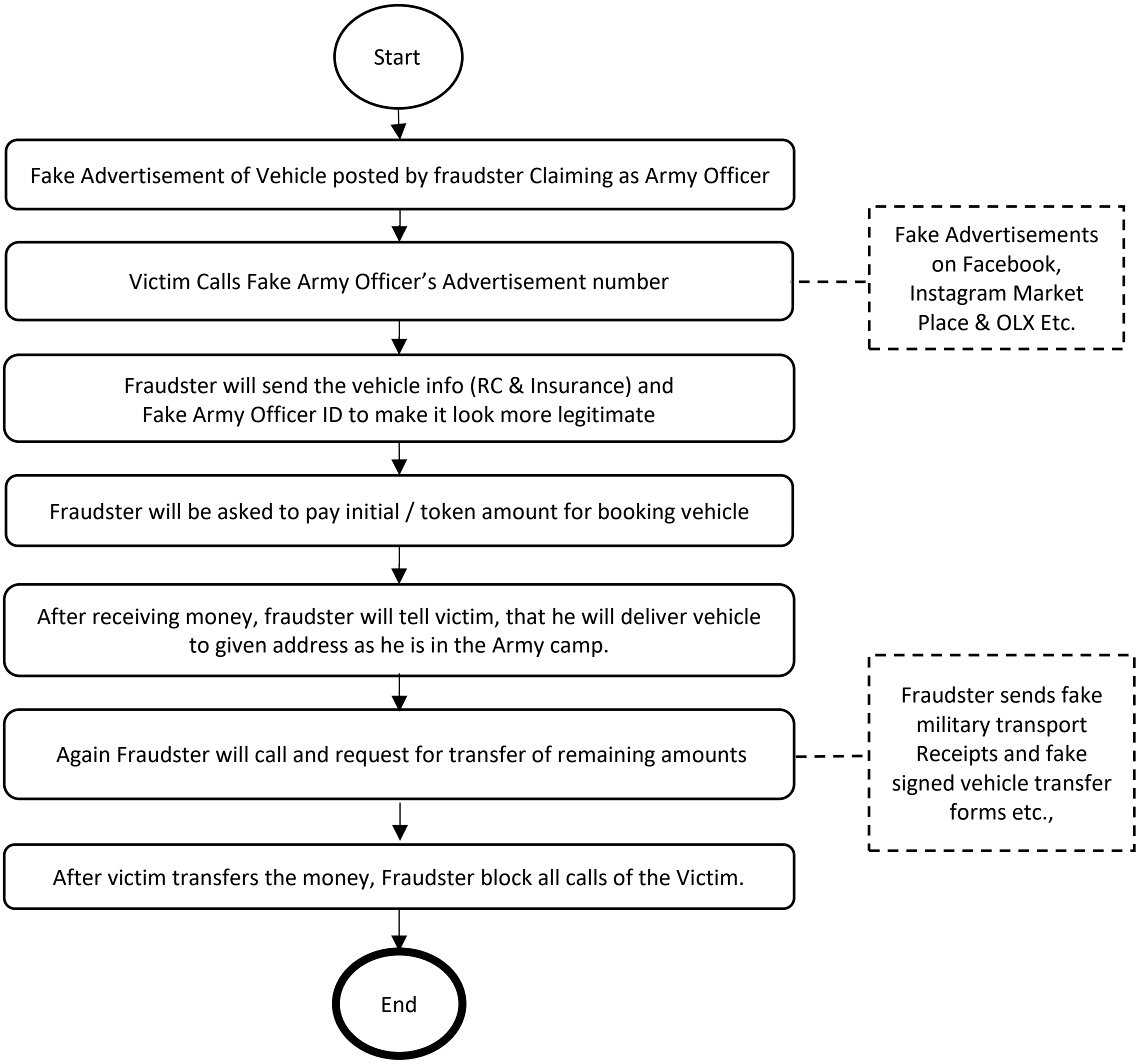
Suspicious User Detected

This person has been removed from OLX. Please don't communicate with the user or exchange any money or items. Contact us for more support

QR Code

Fake Post

Fake Advertisement / OLX Fraud – Flow Chart



Start

Fake Advertisement of Vehicle posted by fraudster Claiming as Army Officer

Victim Calls Fake Army Officer's Advertisement number

Fake Advertisements on Facebook, Instagram Market Place & OLX Etc.

Fraudster will send the vehicle info (RC & Insurance) and Fake Army Officer ID to make it look more legitimate

Fraudster will be asked to pay initial / token amount for booking vehicle

After receiving money, fraudster will tell victim, that he will deliver vehicle to given address as he is in the Army camp.

Again Fraudster will call and request for transfer of remaining amounts

Fraudster sends fake military transport Receipts and fake signed vehicle transfer forms etc.,

After victim transfers the money, Fraudster block all calls of the Victim.

End

6.2 Expected Areas of Evidence:

The digital evidence needs to be collected from service providers for the investigation purpose. Since e-Commerce companies collect user's information for extending their services, including user's addresses, modes of payment, bank details, and purchased item details, the Investigating Officers can collect the following information and digital evidence from them to build a strong case.

- Fake OLX profile registration details (Date, Email ID, Alternate email ID, Mobile No, etc.) with KYC form of accused

- The details of login/logout I.P address along with date and time of online transaction
- Fake ID proof of Army officer
- the specific Location history of the suspect/ accused
- Fake ID proof of Army Officer,
- The Chat History between the victim and accused
- The beneficiary account details and its connected ID proofs etc
- The Geo-Location of the suspect/ accused
- The details of linked Wallets and bank A/Cs

6.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Address a letter to the platform u/Sec 91 Cr. P.C is requesting to furnish the user details who posted the advertisement.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If the fraudster duped the victim by sending a Q.R. code, that means the fraudster holds a merchant account; in such case, serve notice U/Sec 91 Cr. P.C to the wallet and collect Photos, pictures of the store/shop, Geolocation, ID proofs, and Bank account.
- Collect the CDRs& CAFs of the mobile numbers from which calls are received. From the CDRS, trace the suspect's locations and contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- If any other services available are found, serve notice u/sec 91 Cr. P.C and collect the registration details, mobile numbers, email I.D.s, etc.
- Sent letter to Telecom Service providers and OLX India for call data records, customer application, forms, and recharge details of the mobile numbers used the fraud, IP addresses for various logins to post the fake ads on OLX.
- Send a Notice to Bank to provide a Statement of Account to which the victim credited funds.

- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- The analysis of Call Data Records (CDR) and Bank statements to identify the locations of the accused.
- Send seized articles to FSL and obtain the Expert's reports.
- Request the concerned to stop the transactions and initiate refunding the amount to the victim.
- Trace the accused by linking the series of events

6.4 Case Study:

Nature of Offence: OLX Fraud

Case Details: A Victim of the Rangareddy district submitted a petition that he had seen an advertisement on the OLX website for the sale of an Innova car and contacted the seller on his phone number 90660XXXX; the seller told him that the car was at RGI Airport, Hyderabad and asked to speak to one Pooja on 7204XXXXX. When the complainant called her, she said he should first deposit two lakh rupees in a given SBI account. Accordingly, he had deposited the amount in the SBI account. Later, he went to Airport for an inspection of the car. However, the seller could not produce the car at the airport as it was allegedly held in the Cargo area. The following day, the victim received another call from 906600xxxx and asked him to deposit a further sum of Rs. 3.5 lakhs for release of the car from Airport cargo, which he did. The seller informed Car number as AP-09-CU-XXXX and that he was asked to pay a further sum of one lakh eighty thousand rupees on xx-12-2017. On the whole, the victim paid Rs.5,50,000/-. After that, the fraudster blocked his number.

In this case, IO**:**

1. Sent a letter to Telecom service provider to get details of fraudster's mobile numbers such as KYC, CAF, CDR, SDR, and IPDR details.
2. Sent a letter to SBI bank to know the details of beneficiary account and transactions
3. Sent a letter to OLX website seeking advertisement details
4. Sent a letter to the concerned RTO to collect details of the Innova Vehicle
5. Traced the accused based on CDR and OLX registration details.
6. Sent material objects to FSL for an Expert's opinion

ꟸ❈ꟹ

7. GIFT FRAUD

Social Media users often see Giveaways posts on Social Media platforms like YouTube and Instagram. They ask the users to like or comment on the post to win groceries or gain followers or a prize that increases their brand value, and the user will be added to the giveaway's draw list. Several Giveaways do not exist at all. Fake social media influencers create them as it is the easiest way of accumulating social media likes and followers.

This fraud is similar to phishing in that the user feels they are participating in a legitimate giveaway programme to promote their products or services. Pharming is the name given to this practice. In this type of fraud, criminals connect with a victim through phone, e-mail, Social Media, etc.

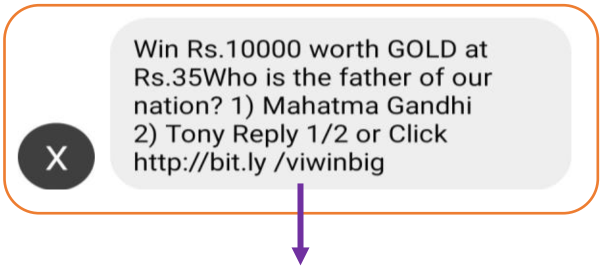
7.1 Modus Operandi:

Fraudsters use official company names, such as the XYZ cosmetic giveaway. However, the XYZ original Company does not offer any giveaways. The fraudster re-edits the profile once the false giveaway page gets targeted likes, subscribers, comments, and shares.

The fraudster will create a short link to the giveaway, or they may install malware to seize user social accounts for a ransom, or they may rename their profile to a different name and sell it to someone looking for an existing page with a higher number of followers/subscribers.

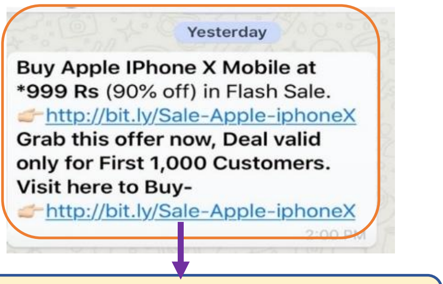
Once the fraudster has amassed the desired number of subscribers/followers, they alter the page's original content and use it for marketing bogus items or selling user data on the dark web, such as name, email address, Aadhar card, Pan Card, DMAT account, etc.

In some cases, fraudsters identify a single woman or widow from matrimonial websites. They introduce themselves as doctors or wealthy businessmen from the UK, USA, etc., and send them fake bio-data. Fraudsters befriend the lady and inform her that he is sending the jewellery as a gift. Later, the victim receives a call from a fake customs officer that a parcel containing jewellery has come, and she needs to pay customs tax to release it. When contacted, the fraudster asks the victim to pay it. Once the amount is paid, the fraudster blocks all the victim's calls.



Win Rs.10000 worth GOLD at Rs.35Who is the father of our nation? 1) Mahatma Gandhi 2) Tony Reply 1/2 or Click http://bit.ly /viwinbig

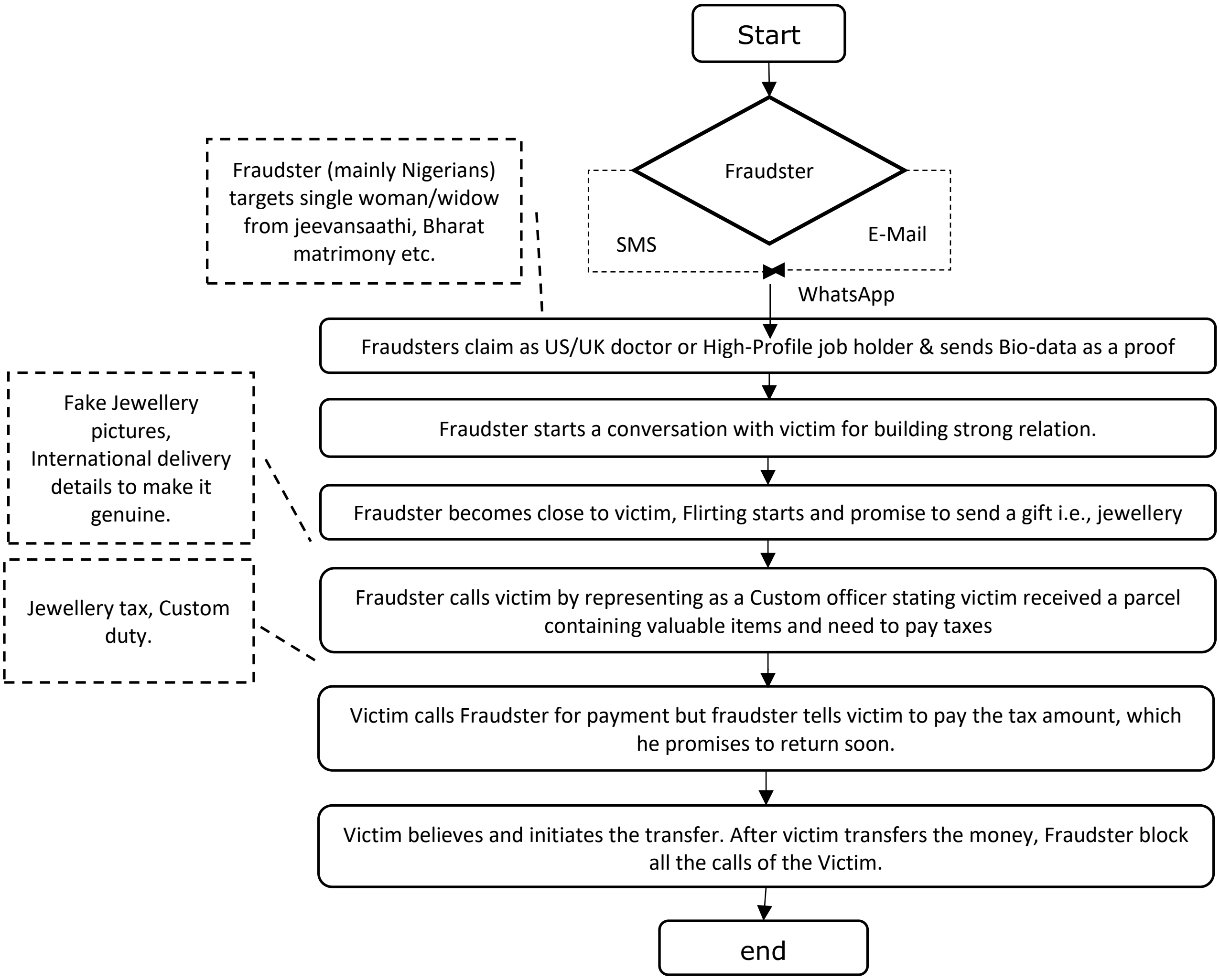
Wrong Claiming and Be Aware of Links



Buy Apple IPhone X Mobile at *999 Rs (90% off) in Flash Sale.
👉http://bit.ly/Sale-Apple-iphoneX
Grab this offer now, Deal valid only for First 1,000 Customers.
Visit here to Buy-
👉http://bit.ly/Sale-Apple-iphoneX

Be aware of links!

Gift Fraud (Matrimonial) Fraud - Flow Chart



Start

Fraudster

SMS

E-Mail

WhatsApp

Fraudster (mainly Nigerians) targets single woman/widow from jeevansaathi, Bharat matrimony etc.

Fraudsters claim as US/UK doctor or High-Profile job holder & sends Bio-data as a proof

Fraudster starts a conversation with victim for building strong relation.

Fake Jewellery pictures, International delivery details to make it genuine.

Fraudster becomes close to victim, Flirting starts and promise to send a gift i.e., jewellery

Jewellery tax, Custom duty.

Fraudster calls victim by representing as a Custom officer stating victim received a parcel containing valuable items and need to pay taxes

Victim calls Fraudster for payment but fraudster tells victim to pay the tax amount, which he promises to return soon.

Victim believes and initiates the transfer. After victim transfers the money, Fraudster block all the calls of the Victim.

end

7.2 Expected areas of evidence:

The IO can collect the following evidence for investigation purposes:

- Social Media platform IDs and screenshots of the conversation
- Registration details of suspects related to Social Media platforms
- Contact details, e-mail ID, FB ID of accused, etc.
- Beneficiary account details
- Transaction particulars and take a screenshot of them.
- Geo-location of suspect/ accused

7.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- If the complainant received any BULK SMS in the name of prize money, then collect the sender of Bulk SMS Ex: QP-SNPDEL from the following link https://www.findandtrace.com/trace-bulk-sms-sender
- Identify the service provider and serve a notice U/sec 91 Cr. P.C to collect the user details, KYC documents, etc.
- In some instances, the accused are using toll-free numbers to contact the public to gain their trust; in such cases, identify the service provider of the toll-free company and serve a notice U/sec 91 Cr. P.C to obtain the user details.
- If any website is used by the accused, find out the domain registrar from whois.domaintools.com and address them with a notice U/sec 91 Cr. P.C requesting to furnish the registrant details & I.P. logs, hosting details, and payment details.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- Collect the CDR (Call Data Records) and CAF (Customer Application Form) of the suspect mobile numbers from which calls were received and linked to the bank account. From the CDRs, trace the suspect's locations and contacts. From the messages/alerts received on the mobile number, trace the banks, websites, or any other services availed by the suspect.

- Search the suspect mobile numbers in open-source tools such as Eyecon and True Caller applications.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify name, bank details & UPI ID if available).
- Initiate the process of refunding the amount to the victim.
- Trace the accused by linking the series of events

7.4 Case Study:

Nature of Offence: On-line Gift Fraud

Brief History of Offence: A 51 years old male Social Worker having a charitable trust reported that he made a friendship with an unknown person on Facebook. After a few days, that person contacted and informed him that he was sending a parcel from Canada with useful items for his trust. After some days, the unknown person informed that the parcel was stopped at the customs office in Delhi Airport for release. The unknown person informed that the parcel contained Hand gloves, Sanitisers, and Face Masks useful during the Covid-19 pandemic. Later, one unknown lady called him and introduced herself as a customs officer at Delhi Airport. She informed that the complainant got one parcel from Canada. For releasing the said parcel, he has to deposit some amount in the given bank account. He had deposited the money in the bank account as per the details furnished by the caller.

Further, on the pretext of various reasons, she asked the complainant to pay multiple charges for releasing the said parcel. As per the caller's direction, he had deposited the amount in the given Bank account. After paying a considerable amount to the fraudster, he realized that he was cheated.

In this case, IO:

1. Collected suspected Mobile numbers & obtained CDR, SDR, and IMEI details from Service Provider
2. Identified the beneficiary account details and froze them
3. Analyzed transactions and further identified the end beneficiaries
4. Collected Facebook ID details from Service Provider
5. Tracked the accused based on IMEI analysis.
6. Sent material objects to FSL for an Expert's opinion

ꕤ

8. LOTTERY FRAUD

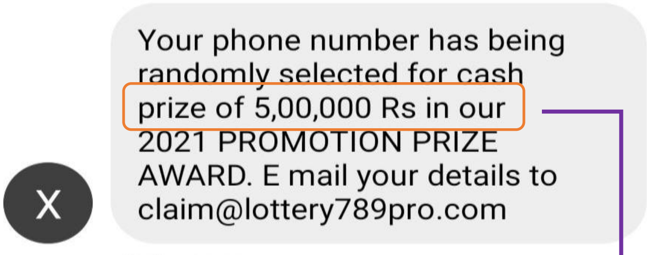
Lottery fraud begins with an attractive e-mail/SMS sent to the victims. Lottery fraudsters will try to convince the victim that he has won the lottery. Then, fraudsters ask the victim to pay advance fees, GST, or income taxes related to the lottery during the process. They will also request personal information on the pretext of verifying identity, but in reality, they will use the information to commit more social engineering crimes.

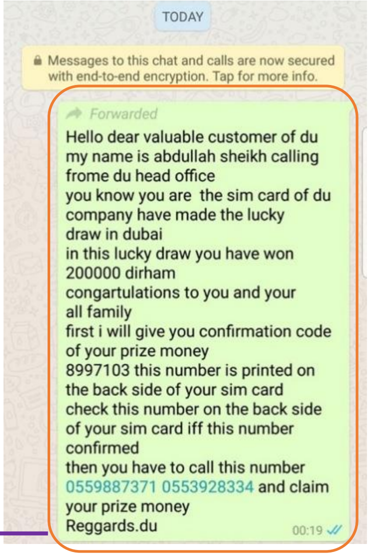
For committing this type of crime, fraudsters use renowned companies' names such as Chevrolet, Amazon, Samsung, etc.

8.1 Modus Operandi:

Fraudsters frequently ask the victim to claim the prize money by calling an automated number, sending a text message to a phone number, or filling out an online form. Fraudsters will try to elicit emotional responses from the victim when interacting with them via email or phone. They will try to gather bank account information, address, credit card information, or personal information.

Fraudsters send couriers, glossy pamphlets, and scratch cards, stating that scratching the card will give them a chance to win the Lottery. The victim is usually the second or third place winner to make it more credible. When the victim tries to call them to claim the prize, the fraudster will demand payment of fees, GST, or income taxes before receiving the award. For this purpose, the fraudsters prepare documents in the name of the Reserve Bank of India, the IT Department, and the Customs Department and send them to the victim.


Your phone number has being randomly selected for cash prize of 5,00,000 Rs in our 2021 PROMOTION PRIZE AWARD. E mail your details to claim@lottery789pro.com


TODAY

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Forwarded
Hello dear valuable customer of du
my name is abdullah sheikh calling frome du head office
you know you are the sim card of du company have made the lucky draw in dubai
in this lucky draw you have won 200000 dirham
congartulations to you and your all family
first i will give you confirmation code of your prize money
8997103 this number is printed on the back side of your sim card
check this number on the back side of your sim card iff this number confirmed
then you have to call this number 0559887371 0553928334 and claim your prize money
Reggards.du
00:19

Lottery prize money.

Fake messages

1 Victims receive emails from fraudster informing that they have won a lottery worth 50 Crores.

2 Victim replies to fraudster on email to complete formalities to get the money.

3 Victim is asked to deposit money for processing fees, Customs clearance, Income Tax authorisation etc.

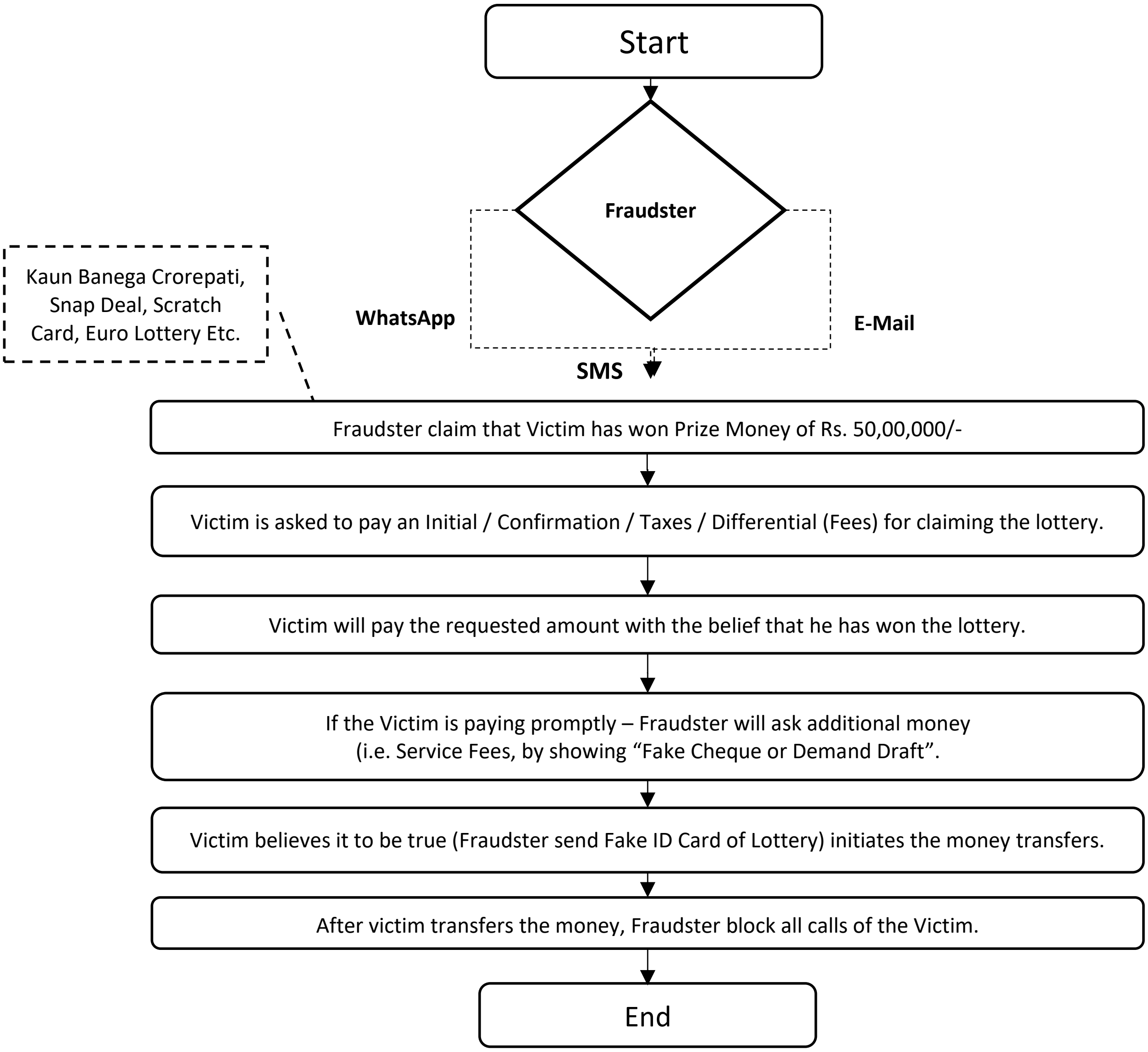
4 Thinking about 50 Crores victim deposits money

5 Victim loses money

The Fraudster will use the following methods to make the victim believe that the lottery is legitimate

- Fraudsters offer bogus vouchers and gift cards via email, text message, or social network message, saying that the victim has won a gift card from a well-known business company.
- Fraudsters make it appear as though the victim is the only one who has won a prize. However, the same text, email, or letter was sent to many people.
- The fraudster imitates legitimate international lottery names and travel prize scams, stating that the victim has won a free vacation, or the fraudster offers incredibly cheap vacation packages that do not exist.
- Telemarketers frequently call to inform that victim has won a free vacation and that he must attend a hotel conference, in which the victim will be urged to pay or join a programme, which is a red flag for a scam.

Lottery Fraud – Flow Chart


Start
Fraudster
Kaun Banega Crorepati, Snap Deal, Scratch Card, Euro Lottery Etc.
WhatsApp
E-Mail
SMS
Fraudster claim that Victim has won Prize Money of Rs. 50,00,000/-
Victim is asked to pay an Initial / Confirmation / Taxes / Differential (Fees) for claiming the lottery.
Victim will pay the requested amount with the belief that he has won the lottery.
If the Victim is paying promptly – Fraudster will ask additional money (i.e. Service Fees, by showing "Fake Cheque or Demand Draft".
Victim believes it to be true (Fraudster send Fake ID Card of Lottery) initiates the money transfers.
After victim transfers the money, Fraudster block all calls of the Victim.
End

8.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to safeguard the integrity of evidence.

The IO can collect the following evidence for investigation purposes-

- The bank account and card data details used for transactions
- Beneficiary account details
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- The names titles used by the fraudsters
- The details of login/logout I.P address along with the date and time of fraudulent transaction
- The Chat History between the victim and accused, if any
- The details of messages and emails
- Screenshots of the fraud transactions
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroboration
- The call recordings between accused and victim, if available on the mobile phone

8.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- If the complainant received any BULK SMS in the name of Lottery money, then collect the sender of Bulk SMS Ex: QP-COCALT from the following link https://www.findandtrace.com/trace-bulk-sms-sender
- Identify the service provider and serve a notice U/sec 91 Cr. P.C to collect the user details, KYC documents, etc.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- Collect the Call Data Records (CDR) of the suspect mobile numbers from which calls were received and linked to the bank account & mail-iD. From the CDRs, trace the suspect's locations and contacts.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.

- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- Initiate the process of refunding the amount to the victim.
- Trace the accused by linking the series of events

8.4 Case Study:

Nature of offence: Lottery fraud

Case details: The complainant received a phone call; the caller introduced himself as a Customer care executive and stated that her mobile number won Lucky Lottery from Airtel Cellular Company India, Mumbai, for Rs 50 Lakhs. For which he asked her to pay Rs. 8000/- towards changing the pin code of her address. Believing his version, she transferred an amount of Rs 8000/- through NEFT from her Account. After paying the amount again on the same day, the executive called her and asked her to pay Rs 18,200/- towards Income Tax. She sent the amount through NEFT to the given account. The following day, he called from the same number and asked her to pay Rs 1000/- for income tax, this time, they gave another account, and she sent the amount through NEFT. The next day executive called her and told her to transfer an amount of Rs 17,200/- for changing the name in the Cheque. From 13th Dec.2016 onwards, she received calls from another mobile no. When she asked for the lottery money, he told her that she would receive the lottery Cheque after paying the amount as told by them. Like that, she paid an amount of Rs.4,09,000/-, but the Executive did not send any amount to her account. Instead, he called her and asked her to pay more to receive her Lucky Lottery amount, showing various reasons.

In this case, IO:

1. Collected the details of the Mobile Numbers of the Suspects/ accused
2. Obtained CDR, SDR, IMEI of Suspect numbers
3. Collected transaction details from Victim's account
4. Obtained beneficiary account details (The money was transferred to 5 accounts)
5. The accused person was traced based on KYC details obtained from the bank.
6. Sent material objects to FSL for an Expert's opinion

ꕥ

9. E-COMMERCE FRAUD

With the advent of the internet, users can send their money anywhere in the world to purchase any product. At the same time, the opportunities for e-commerce fraud also increased. Some customers who purchased through e-Commerce websites (Amazon, Flipkart, Snap deal, etc.) claimed to have received stones instead of iPods and Soap bars instead of phones.

In recent times, social engineering crimes committed by fraudsters by impersonating buyers and sellers, online shopping frauds have increased manifold. Fraudsters use phishing emails to deceive customers into divulging their account names and passwords. This can be done by email or other inventive means.

The fraudsters use gathered information to log into a customer's account, change the password and delivery address, and make unauthorized purchases. This type of scam can go unnoticed for some time due to a lack of awareness on the part of the customer.

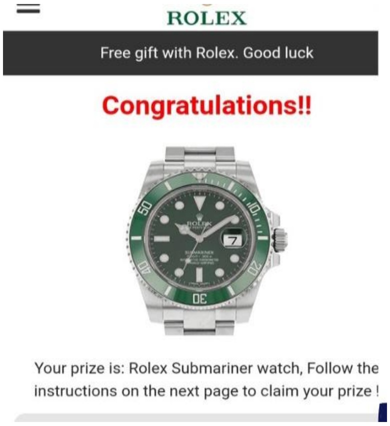
9.1 Modus Operandi:

Fraudsters impersonate themselves as Defence Personnel posing as buyers as well as sellers.

A fraudster impersonating as a member of the armed forces and contacting as a seller: The fraudster's method is to publish false ads for cars and motorcycles with attractive prices, then provide bogus defense (Army, CISF, CRP) identity papers to earn the victim's trust. The fraudster will ask for a token amount of advance money for the merchandise, couriers/transportation charges, and after gaining the victim's trust. Once the money is received, all further calls and messages will be blocked.

A fraudster impersonating as a member of the armed forces and contacting as a buyer: Fraudsters will approach as buyers and readily agree to the victim's asking price without bargain. They will make a little payment via UPI applications to build the victim's trust and pose as a legitimate buyer. The Fraudster will send a QR code for a larger amount and asks the Victim to scan it. After the victim scans the QR code, the fraudster will remove money from the account. Sometimes, the fraudster emails a link or a Google form requiring the victim to fill in UPI / OTP information.

QR Code



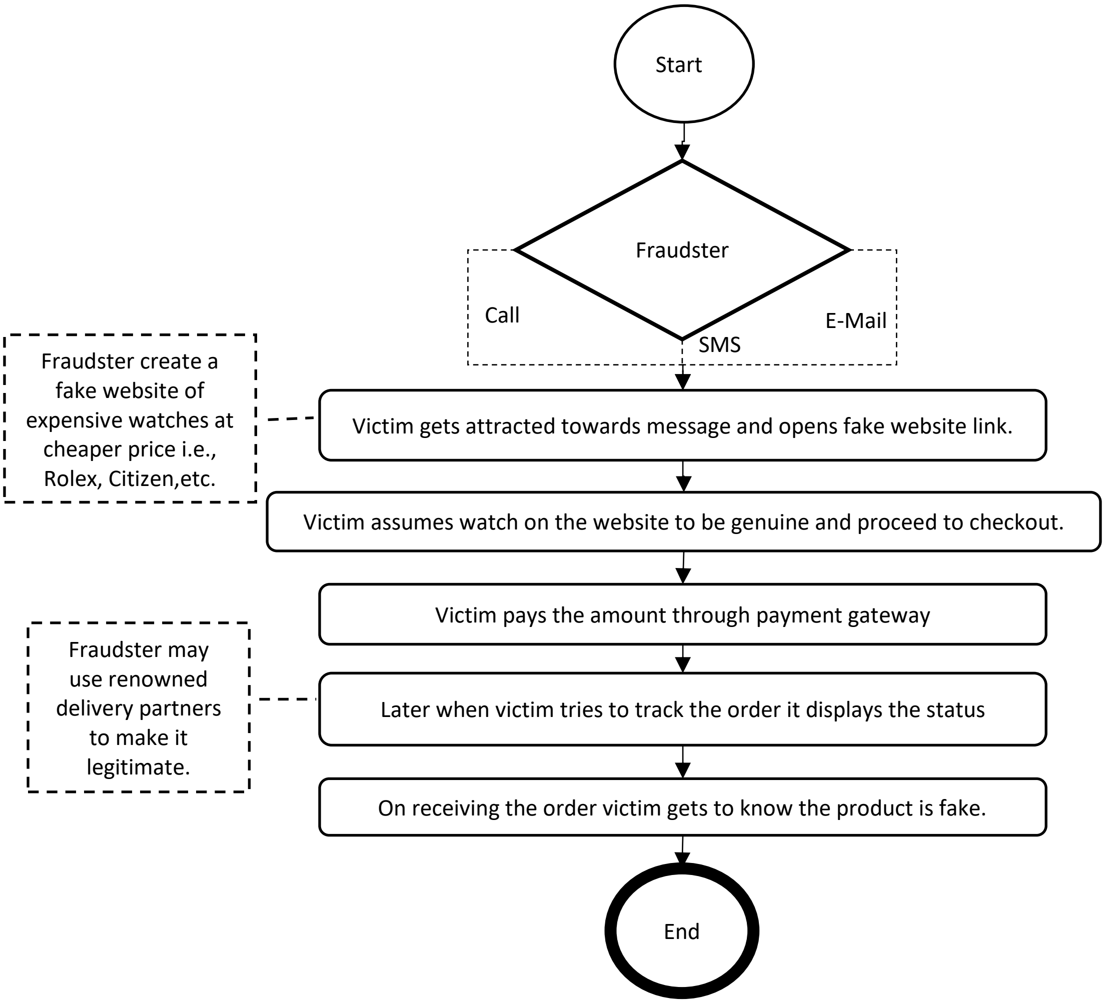
ROLEX

Free gift with Rolex. Good luck

Congratulations!!

Your prize is: Rolex Submariner watch, Follow the instructions on the next page to claim your prize !

E-commerce Fraud - Flow Chart



Start

Fraudster

Call

SMS

E-Mail

Fraudster create a fake website of expensive watches at cheaper price i.e., Rolex, Citizen,etc.

Victim gets attracted towards message and opens fake website link.

Victim assumes watch on the website to be genuine and proceed to checkout.

Victim pays the amount through payment gateway

Fraudster may use renowned delivery partners to make it legitimate.

Later when victim tries to track the order it displays the status

On receiving the order victim gets to know the product is fake.

End

9.2 Expected Areas of Evidence:

The IO can collect the following evidence for investigation purposes:

- The bank account and credit card data used for transactions.
- The names and titles used by the fraudsters.
- The details of messages and emails.
- Open the victim's account, collect screenshots of the fraud transactions
- In Bank Statement – Highlight the concerned transactions for further analysis
- The call recordings, if available on the mobile phone
- The beneficiary accounts details
- The Payment gateway details
- Invoice copy of order and delivery
- Mobile Number and e-mail ID of accused
- Fake website link on Google

9.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find the websites involved, find out the domain registrar from an open-source tool whois.domaintools.com which tells about the registration date, IP address, Location of the server, and registrar's information.
- Address a notice u/sec 91 Cr. P.C requesting to furnish the registrant details & I.P. logs, hosting details, and payment details.
- Check to which account the money has been transferred and what payment gateway the website is using, and contact the payment gateway that has been associated with the transaction.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Contact the specific bank to keep the suspected account on the block list.
- Ask the victim to change their credentials for bank accounts
- Initiate the process of refunding the amount to the victim.
- Trace the accused by linking the series of events

9.4 Case Study:

Nature of Offence: E-Commerce Fraud

Case Details: A complainant aged: 24 years, resident of Hyderabad, reported that in the last three days, some unauthorized persons placed several orders on e-commerce sites of inner garments of females & males and condoms to her address and harassed her mentally. They are placing orders from websites such as Zivame.com, bewakoof.com, and amazon.com using her email IDs and mobile numbers. They are trying to log in to her online accounts and reset their password. They are creating new accounts and placing orders for her. All orders are placed on cash and delivery method.

In this case, IO:

1. Sent Notice u/s 91 Cr.P.C. to concerned E-Commerce Websites for providing the IP logs for the fake deliveries being placed and obtained the details.
2. Analyzed the IPs and sent Notices U/s. 91 Cr.P.C. to concern ISPs being used by the accused to place the fake orders and collect the internet connection address.
3. Traced out the accused person's details based on the IP location and arrested.
4. Sent material objects to FSL for an Expert's opinion

10. QR CODE FRAUD

The country is rapidly moving toward a cashless economy. Digital transactions have made life easier by eliminating the need to travel to pay cash or log on to the internet to complete NEFT or RTGS transactions. Unified Payment Interface (UPI) is a quick way to make a digital payment gaining popularity.

In recent years, UPI has become one of the most popular payment systems. Simply scan a QR code and enter a four-digit PIN to authorize a financial transaction, and the entire transaction is completed in seconds. The Popular payment apps which use QR codes are Google Pay, Paytm, PhonePe, Bhim App, MobiKwik, PayzApp, Razorpay, etc.

A Quick Response (QR) code is a scannable barcode encoded with data. Fraudsters create their QR code to steal banking or personal information and receive money from the victims in a fraudulent manner.

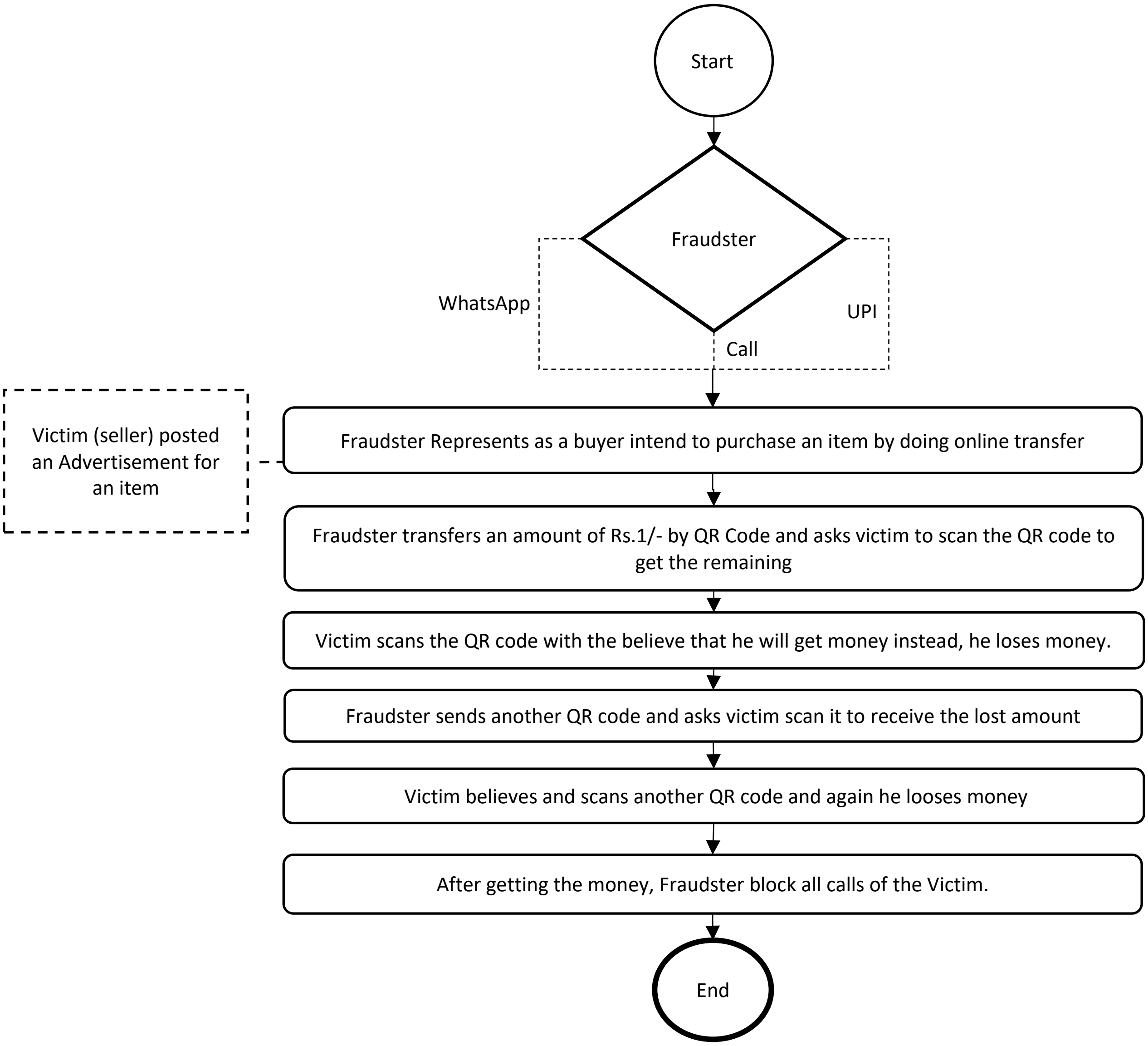
When someone posts an item for sale on an online auction platform, the fraudsters pose as buyers, generate a QR code, and send it via WhatsApp or email to the chosen victim. They will instruct the victim to scan a QR code to receive money immediately into their bank accounts. Victims scan QR codes sent by fraudsters, believing that money will be deposited into their accounts; instead, they lose money.

10.1 Modus Operandi:

Fraudsters have found new, creative ways to commit fraud, to make it believe legitimate. One way of doing this is by sending people texts messages. Such as congrats on winning Rs 5,00,000 along with the picture of a QR code. The message will lure the victim into scanning the code and entering the amount, followed by UPI PIN to receive the cash into the account. Victims believe that money will be credited into their accounts. But money is deducted from the account instead of receiving it.

Another method includes false QR codes in phishing emails, texts, or social media posts. After scanning the false code, users are routed to websites with realistic-looking pages, where the victim may be invited to log in by providing PII (Personally Identifiable Information)

QR Code Fraud - Flow Chart



Victim (seller) posted an Advertisement for an item

Fraudster Represents as a buyer intend to purchase an item by doing online transfer

Fraudster transfers an amount of Rs.1/- by QR Code and asks victim to scan the QR code to get the remaining

Victim scans the QR code with the believe that he will get money instead, he loses money.

Fraudster sends another QR code and asks victim scan it to receive the lost amount

Victim believes and scans another QR code and again he looses money

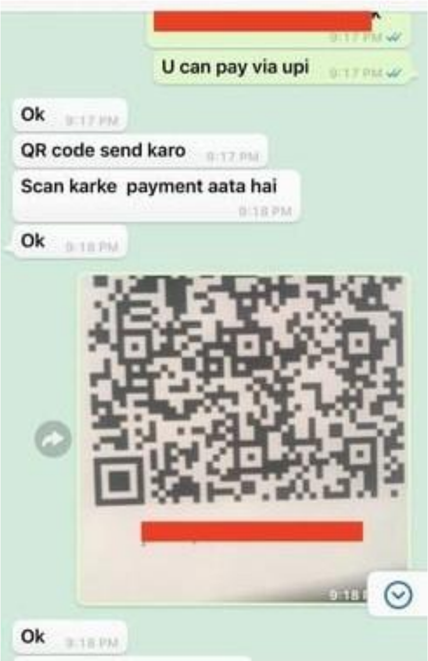
After getting the money, Fraudster block all calls of the Victim.

10.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to safeguard the integrity of evidence.

The IO can collect the following evidence for investigation purposes:

- The chat if the QR code is sent through WhatsApp or Instagram/ Facebook
- The bank account and credit card data used for transactions.
- The screenshots of fraudulent UPI Transaction Details.
- The details of login/logout I.P address along with the date and time of fraudulent transaction
- The specific Location history of the suspect/ accused
- The Chat History between user & accused
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroborations.
- The call recordings, if available on the mobile phone
- Details of the beneficiary account.



[redacted]
9:17 PM

U can pay via upi 9:17 PM

Ok 9:17 PM

QR code send karo 9:17 PM

Scan karke payment aata hai 9:18 PM

Ok 9:18 PM

[redacted]
9:18

Ok 9:18 PM

10.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find out from which phone number the victim has received the QR code.
- Check the victim's bank statement and determine when and how the withdrawals took place.
- Identify to which suspect account the money has been transferred.
- Contact the concerned bank and ask them to stop the transaction and block the suspect account.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Ask the victim to change their credentials for bank accounts.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts.
- Request the concerned to stop the alleged transactions and initiate the process of refunding the used amount.
- Trace the accused by linking the series of events

10.4 Case Study:

Nature of Offence: QR Code Fraud

Case Details: The complainant stated that he works as a carpenter. He received a call from 639298XXXX. The accused introduced himself as a furniture painter. The accused said that his Phonepe app is not working on accepting payment from customers, so the accused wants to give the complainant’s mobile number to various customers. Later the accused sent a QR code worth Rs. 24,999/- through WhatsApp no:701487XXX to the complainant and asked him to scan it four times, So that the amount would be credited into the complainant's account. Believing the accused as genuine, the complainant scanned the QR codes two times and lost Rs.50,000/-. When the complainant asked about money deductions to the accused, he stopped responding to the complainant's calls/messages.

In this case, IO:

1. Collected the offense-related documents from the complainant and sent notice U/s 91 Cr. P.C to Airtel Payments Bank and Paytm No: 639XXXX for beneficiary details.
2. Sent a requisition to Telecom Service Providers to furnish CDR, SDR, and CAF of mobile numbers
3. Identified the locations of the accused and also collected the Photo of the accused through Bank KYC
4. Based on the location history, the accused was traced.
5. Sent material objects to FSL for an Expert’s opinion

The main challenge found during the investigation of the case is that the address provided by the accused to the bank is fake, making the identification of the victim difficult.

ꕥ✵ꕥ

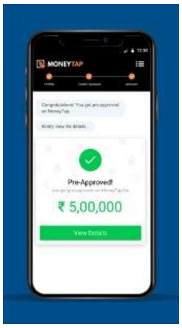
11. ONLINE LOAN FRAUDS

The want for personal loans and finance to stream the short-term crisis has increased rapidly. Personal loans are in demand for various reasons, including the revival of business and repayment of other loans. However, this want has also given rise to several incidents of fraud. Fraudsters have taken advantage of those in need and have robbed the victims of their hard-earned money.

Personal Loans and Fake Instant Personal Loans are offered through SMS/WhatsApp or Loan Apps. Illegal smartphone loan apps are spread over various application stores. And fraudsters are committing offences through these apps. Loan offer frauds affect common people looking for loans, giving them false hope of providing hassle-free instant loans at lower interest rates without any documentation.

Types of Loan Frauds:

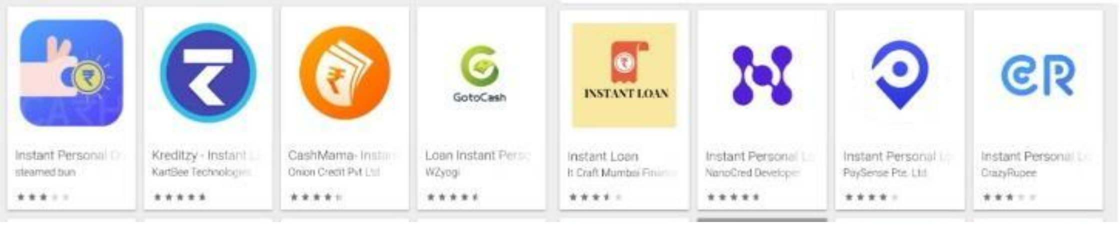
Fake Corporate Agents Loan Frauds:



Fraudsters make random calls or send SMS/WhatsApp about the loan, and the victims are lured into sending their credentials. Next, the victim receives a Verification Completeness Certificate and a scanned copy of the Cheque. Fraudsters then lure the victim into sending 10% GST and another 10% Support/Processing Fees and courier charges.

Fake Identity Personal Loan Frauds:

Fraudsters with PAN/Aadhar cards of Victims apply for loans while concealing their identities with modified images. They also open a bank account with fake details and apply for loans. Once the loan is approved, the fraudster cuts off all his communication. Typically, victims learn about this when they apply for a new loan and discover that someone else has already taken a loan in their name (As reflected in CIBIL). Victims are frequently contacted by collection agents who demand payment of EMI amounts.



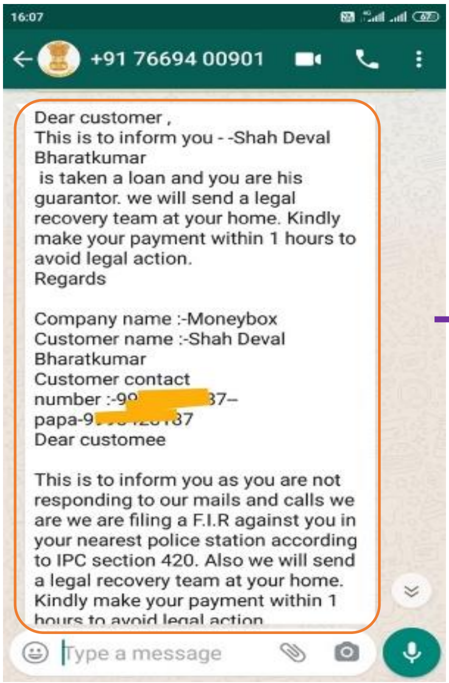
Instant (App based) Loan Frauds:

It's a scam where illegal lenders offer immediate personal loans through mobile apps at high-interest rates. After uploading personal information, a copy of the Aadhaar card, and the PAN card to the App, a customer can get a loan in minutes. Loans ranging from Rs 1000 to Rs 50,000 are available for a week or short period. The majority of the apps available on the Google Play Store have no affiliation with any Bank or Non-Banking Financial Institution.

The interest rate of these loans is very high; Tele-callers and recovery employees will communicate with borrowers from the lending corporations' call centers for recovery of loans.

11.1 Modus Operandi:

- While installing the Loan App from the play store, the app demands access to the customer’s gallery, contacts, phone book, messaging, and location services
- The customer must submit a photo ID, Aadhaar card, PAN Card and upload a selfie/photo from the registered mobile
- Loans usually get approved after the completion of electronic authentication
- Loan ranges from Rs. 500 to Rs. 50,000, which will be sanctioned instantly. The loan amount will be given after the deduction of interest.
- If a consumer fails to repay a loan on time, the lender will pursue it aggressively.
- The Tele-callers (fraudsters) use a combination of coercion, blackmail, and threats and levy high penalties for failure or delay in the loan payment.
- The customer will be harassed with dozens of calls.
- If not paid in time, abusive calls will be made to the customer’s family members, and threats and blackmail will start.
- Finally, they gain access to the contacts of the customers' relatives and friends and send them defamatory WhatsApp messages about the defaulter.
- Fraudsters also send fake FIR/Lawsuits to the victims.



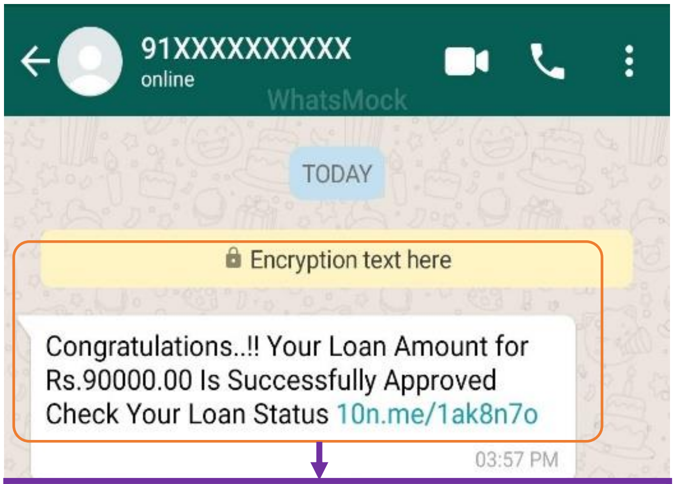
16:07

+91 76694 00901

Dear customer ,
This is to inform you - -Shah Deval Bharatkumar
is taken a loan and you are his guarantor. we will send a legal recovery team at your home. Kindly make your payment within 1 hours to avoid legal action.
Regards

Company name :-Moneybox
Customer name :-Shah Deval Bharatkumar
Customer contact number :-99[redacted]37–
papa-9[redacted]87
Dear customee

This is to inform you as you are not responding to our mails and calls we are we are filing a F.I.R against you in your nearest police station according to IPC section 420. Also we will send a legal recovery team at your home. Kindly make your payment within 1 hours to avoid legal action



91XXXXXXXXXX
online

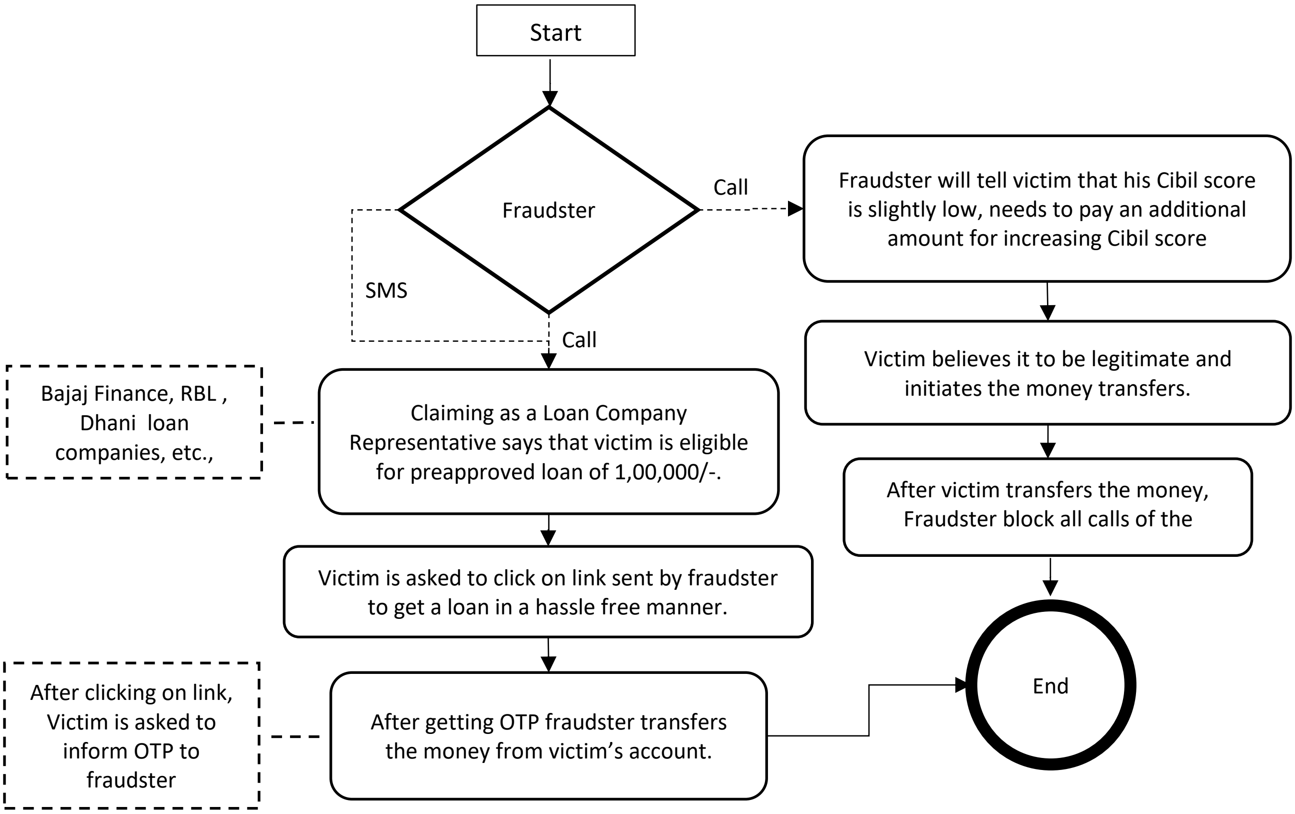
Congratulations..!! Your Loan Amount for Rs.90000.00 Is Successfully Approved Check Your Loan Status 10n.me/1ak8n7o

03:57 PM

Claiming that one has eligibility to get loan.

Fake loan messages claiming that is from government.

Loan Fraud - Flow Chart



Start
Fraudster
Call
SMS
Call
Fraudster will tell victim that his Cibil score is slightly low, needs to pay an additional amount for increasing Cibil score
Victim believes it to be legitimate and initiates the money transfers.
After victim transfers the money, Fraudster block all calls of the
End
Bajaj Finance, RBL , Dhani loan companies, etc.,
Claiming as a Loan Company Representative says that victim is eligible for preapproved loan of 1,00,000/-.
Victim is asked to click on link sent by fraudster to get a loan in a hassle free manner.
After clicking on link, Victim is asked to inform OTP to fraudster
After getting OTP fraudster transfers the money from victim's account.

11.2 Expected Areas of Evidence:

The IO can collect the following evidence for investigation purposes:

- The account holder's name, statement of the account
- The scanned copy of the account opening form along with documents submitted as proof of identity & address
- The registered mobile number, email address, other proofs linked to the account
- Fake website link, Mobile Number, and e-mail address of accused
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- The names, titles used by the fraudsters
- Details of the messages
- Open the victim’s account, collect screenshots of the fraud loan payment transactions
- Details of the beneficiary account
- In Bank Statement – Highlight the concerned transactions for further analysis
- The call recordings, if available on the mobile phone
- The details of Login/Logout IPs of the transaction
- In case of money withdrawals, Collect the CCTV footage if available, i.e., Bank and ATM

11.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Analyze the victim’s bank statement and find the beneficiary Accounts.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If the complainant received any BULK SMS in the name of a loan, then collect the sender of Bulk SMS Ex: QP-AMLOAN from the following link https://www.findandtrace.com/trace-bulk-sms-sender
- Identify the service provider and serve a notice U/sec 91 Cr. P.C to collect the user details, KYC documents, etc.
- If the complainant received any mails, serve a notice U/Sec 91 Cr. P.C to the mail service provider and collect the registration details, I.P. logs, registered mobile number, recovery mail ID, etc.

- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- If any sites are involved, find out the domain registrar from whois.domaintools.com and address a notice u/sec 91 Cr. P.C requesting to furnish the registrant details, control Panel & I.P. logs, hosting details, and payment details.
- Collect the Call Data Records (CDR) of the suspect mobile numbers from which calls were received and linked to the bank account & mail-ID. From the CDRs, trace the suspect's locations his contacts.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- If any private company is involved in the above fraud, collect company details from https://www.mca.gov.in/mcafoportal/showCheckCompanyName.do.
- Trace the accused by linking the series of events

11.4 Case Study:

Nature of Offence: Loan Apps Fraud

Case Details: The complainant reported that on 18th Nov 2020, he had taken a loan of Rs.3,500/- from one App, "**My Bank**" and within one week, he paid the amount. Later he took a loan of Rs.4,500/- from the same Loan App, and again, he paid the amount. Later, when he verified his bank statement (SBI Bank), he found an amount of Rs. 26,000/- was credited to his bank account from 14 different Loan applications, i.e., Bubble loan, Rupee Bazar, Ok cash, rupee factory, Paisa Loan, One hope, Cash bee, In Need, Snapit loan, Piggybank, Krazy Rupee, Real Rupee/Rupee Bear, Rupee Most without his request, for which he paid Rs.44,000/-(Approx.) to said loan apps. But said apps continuously credited amounts to his account without his consent and harassed him to repay excess amounts. In this way, the complainant was forced into "DEPT TRAP" by these microfinance loan apps and harassed him for repayment, levying an abnormal interest rate. Complainant on enquiry came to know that they were running the non-banking finance businesses without valid licenses from RBI/concerned Govt. authorities. They collect the contact details and photos from the borrowers while sanctioning the loans. After approving the loans, they are asked to repay within seven days, including a higher interest rate. They are making calls to the persons in the contact list of the complainant and spreading bad propaganda against him as a fraud and defaulter by using abusive language.

In this case, IO:

1. The accused persons used VOIP numbers and WhatsApp for calling the victims
2. I.O. sent a 91 Cr.P.C. notice to the law enforcement department of WhatsApp www.whatsapp.com/records for IPs of the VOIP numbers and obtained the details.
3. IO. Sent 91 Cr.P.C. notices to concerned ISPs to provide internet connection details of the fraudster.
4. Collected the details of the accounts from which the loan amount was credited to the complainant's SBI account
5. After receiving Internet connection details accused was traced and arrested.
6. Sent material objects to FSL for an Expert's opinion

12. SIM SWAPPING FRAUD

A mobile number could provide a way for cybercriminals to access financial accounts. Mobile phones are jam-packed with information from contact lists, images, emails, and Short Message Services (SMSs) to financial details like ATM withdrawal alerts and one-time passwords (OTPs) issued by banks for net banking transactions. SIM swapping relies on phone-based authentication.

Fraudsters use new SIM cards for committing fraud and withdrawing money from the victim's account. In SIM swap fraud, fraudsters take a new SIM from the Service Provider with the victim's phone number on some pretext e.g., SIM Card lost or damaged. Thereby, the fraudster gets access to the victim's OTPs and card-related alerts once SIM is swapped.

12.1 Modus Operandi:

Fraudsters impersonate customers and call cell carriers, stating that their (Victim's) SIM card has been misplaced or damaged. They then request that the customer support professional activate a new SIM card. This forwards the customer's phone number to the fraudster's smartphone, equipped with a different SIM card. Criminal use forged documents of the victim to apply for a duplicate SIM Card.
This fraud has two stages: net banking fraud and SIM swap.

Net Banking Frauds

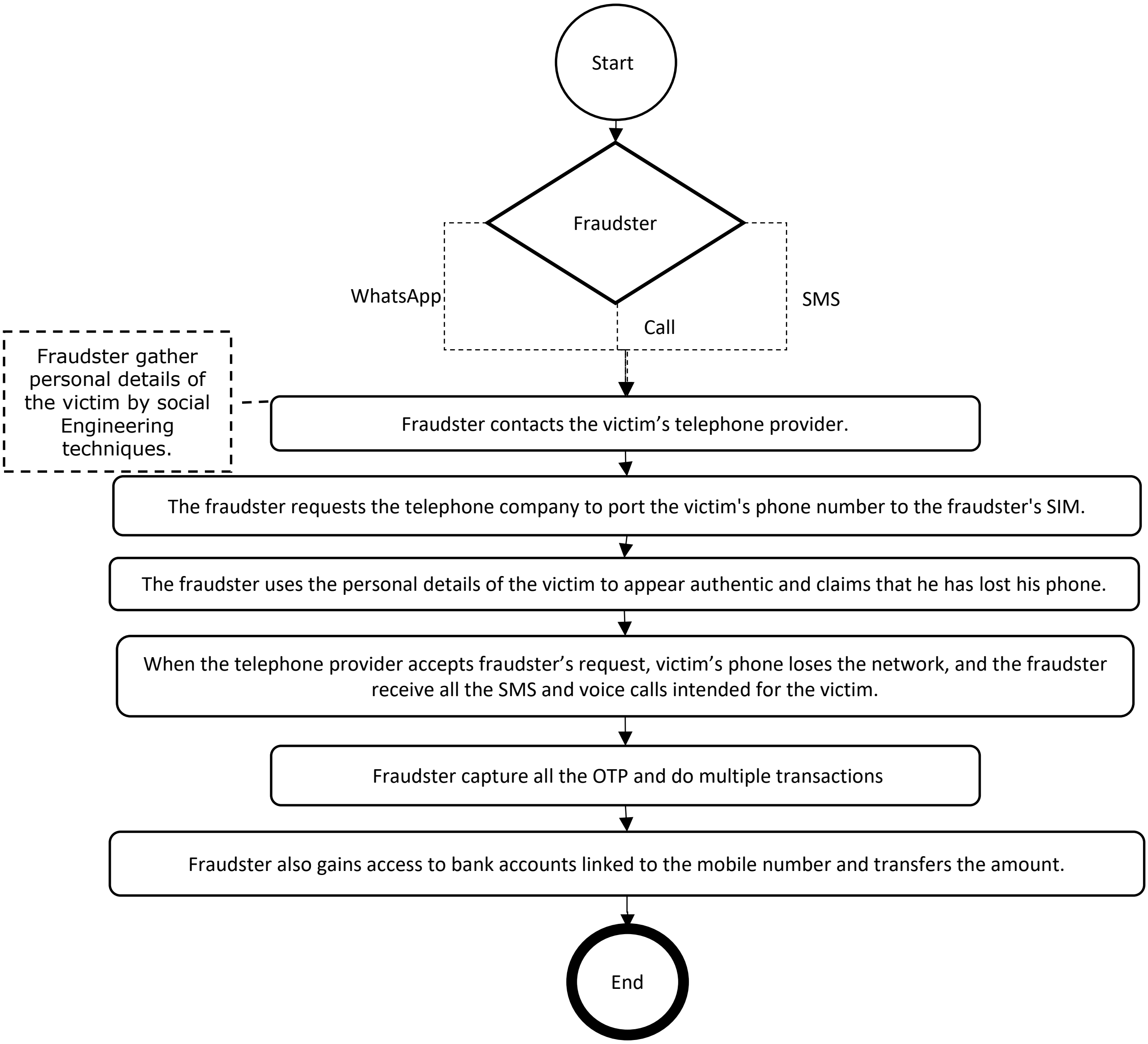
Fraudsters deliver a seemingly harmless Trojan or malware on customers' devices to access their bank account and mobile number information. Then they call the customer and pretend to be service provider agents, asking for personal information. Furthermore, many naive victims readily reveal the facts without hesitation.

SIM Swap Fraud

The fraudster approaches the service provider with forged documents and requests a SIM swap. The service provider deactivates the previous SIM in the victim's phone. A fresh active mobile SIM card is given to the fraudsters. This makes the victim's SIM card without a network. Then, all of the victim's financial SMSs, (OTP) one-time password notifications, and other financial alerts or transaction confirmations were received on the new active card, which fraudsters use to commit fraud.

This is a two-step fraud in which the fraudsters first obtain victims' bank account information using phishing emails, malware, or Trojans, and then use the SIM switch technique to block the victim's SIM. By the time victim learned about the SIM Swapping request from Service Provider, the fraudsters might have taken money from the victim's bank account.

SIM Swapping Fraud - Flow Chart


Start
Fraudster
WhatsApp
Call
SMS
Fraudster gather personal details of the victim by social Engineering techniques.
Fraudster contacts the victim’s telephone provider.
The fraudster requests the telephone company to port the victim's phone number to the fraudster's SIM.
The fraudster uses the personal details of the victim to appear authentic and claims that he has lost his phone.
When the telephone provider accepts fraudster’s request, victim’s phone loses the network, and the fraudster receive all the SMS and voice calls intended for the victim.
Fraudster capture all the OTP and do multiple transactions
Fraudster also gains access to bank accounts linked to the mobile number and transfers the amount.
End

12.2 Expected areas of evidence.

The IO can collect the following evidence for investigation purposes:

- Based on the SIM number, try to find details of criminal
- If mobile is switched OFF, request service provider for CDR and last location
- If mobile is ON, request Service Provider for the current location of the suspect/accused.
- Documents submitted by the accused to Service Provider for SIM Swap

- Analyze the IMEI number of criminals to know the location and other numbers used by the criminal
- Beneficiary account details

12.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Find out the victim's messages by mobile service providers like Vodafone, Airtel, IDEA, etc.
- Collect information regarding the fraudsters as to how they purchased a new SIM Card.
- Serve a notice U/sec 91 C r.P.C to the nodal team and collect the details like phone number and device details of the accused, from which they communicated to the victim.
- Collect the CCTV footage of the shop or repair center and surroundings from which a new SIM card has been issued to the fraudster.
- Try to find out the persons who have swapped the SIM. Find out from which shop or repair center. They are running this fraud.
- Look if the fraudsters use any bikes/four-wheelers in the CCTV footage.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Take screenshots of transaction details and identity the beneficiary
- Trace the accused by linking the series of events

12.4 Case Study:

Nature of Offence: SIM Swapping

Case Details: Complainant reported that he has a Saving A/c No.520045XXXXX in SBI Bank, Ramanthapur branch, and two accounts in Oriental Bank of Commerce Bank at Auto Nagar, Ranga Reddy Dist. The mobile No. 924650XXX IDEA was registered to all the above accounts for communication and transactions purpose. He also got registered his Email ID to the SBI account. He got registered mobile no.800814XXXX as a secondary mobile number to his OBC Bank Saving account. On 15-1-2020 morning, he found his IDEA mobile no. 924650XXX has been disabled and not functioning. When he called IDEA customer care, they informed the complainant that a new SIM was taken in his name as the SIM card was lost. On 16-1-2020, he received an SMS from OBC Bank on a secondary mobile number that Rs. 20,00,000/- was withdrawn from his account. Again, the fraudsters have withdrawn an amount of Rs. 25,16,000/- from victims' OBC accounts.

In this case, IO:

1. Verified the bank statement of the complainant’s bank account and identified that amount had been transferred into four accounts of West Bengal State
2. Obtained KYC particulars, account opening form of beneficiary accounts
3. Verified the addresses of the account holders and arrested one of the account holders
4. Collected the fake documents submitted by the fraudster to Service Provider for SIM Swap.
5. The main challenge in the investigation was that the beneficiary account holders were spread across different districts of West Bengal.
6. Sent material objects to FSL for an Expert’s opinion

ജ☼ഓ

13. SOCIAL MEDIA-BASED FRAUDS

In the era of digital technology, Social Media such as Facebook, Twitter, and LinkedIn have become key tools in conducting various activities in our day-to-day lives. Fraudsters choose Social Media to appear legitimate and to reach people easily. We live in a time where privacy seems to be eroding as more and more technologies are integrated into our daily lives. Inappropriate use of our data has become a topic of significant importance in recent years. Whether it's phishing assaults, protecting business accounts from intrusion, battling fraud, or defending against social engineering like mimicking accounts, social media comes with its own set of threats.

Social media accounts are vulnerable to exploitation; common attacks include (a) Hashtag Hijacking, (b) Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), (c) Pharming, (d) Phishing and Clickjacking, (e) Identity Theft and (f) Impersonation, all of which involve the risk of losing something valuable (i.e., information, reputation, or goodwill)

13.1 Modus Operandi:

For fraudsters, social media fraud is a lucrative source of cash. They use social media platforms like Facebook and Twitter to entice victims by appealing to their emotions and offering a gift or unique offer. The post's link leads to a website that asks for personal information or infects the computer with malware that captures the victim’s complete contact list and sends messages to all contacts. Because the communications come from someone they know and trust, they are more likely to click on the link, leading to malware being downloaded unwittingly.

The fraudsters resort to the following methods:

Advertisement Frauds – Copy Products (Replica) are displayed and sold in Social Media Market Places, which are attractive destinations for fraudsters. (For example) in jolly fashion.com, fabricmaniaa.com, fabricwibes.com, takesaree.com, republicsaleoffers.myshopify.com, etc.,

Job Frauds "Open to Work" – Job portals are frequent destinations for fraudsters; they hunt for people with an open-to-work status and use social engineering methods to trick unsuspecting people into paying registration and backdoor fees for employment sites that don't have a fact-checking feature.

Money Double Frauds – We frequently see posts offering to give 2000-3000 INR a day, and they often imitate popular stores such as Amazon, Snapdeal, Naaptol, and Jabon. Victims purchase a virtual product with a virtual value displayed on a website (No Physical Product). Anyone who purchases this product through a recommendation will receive referral margins, which will be added to the virtual value. The virtual money that has been displayed cannot be withdrawn indefinitely.

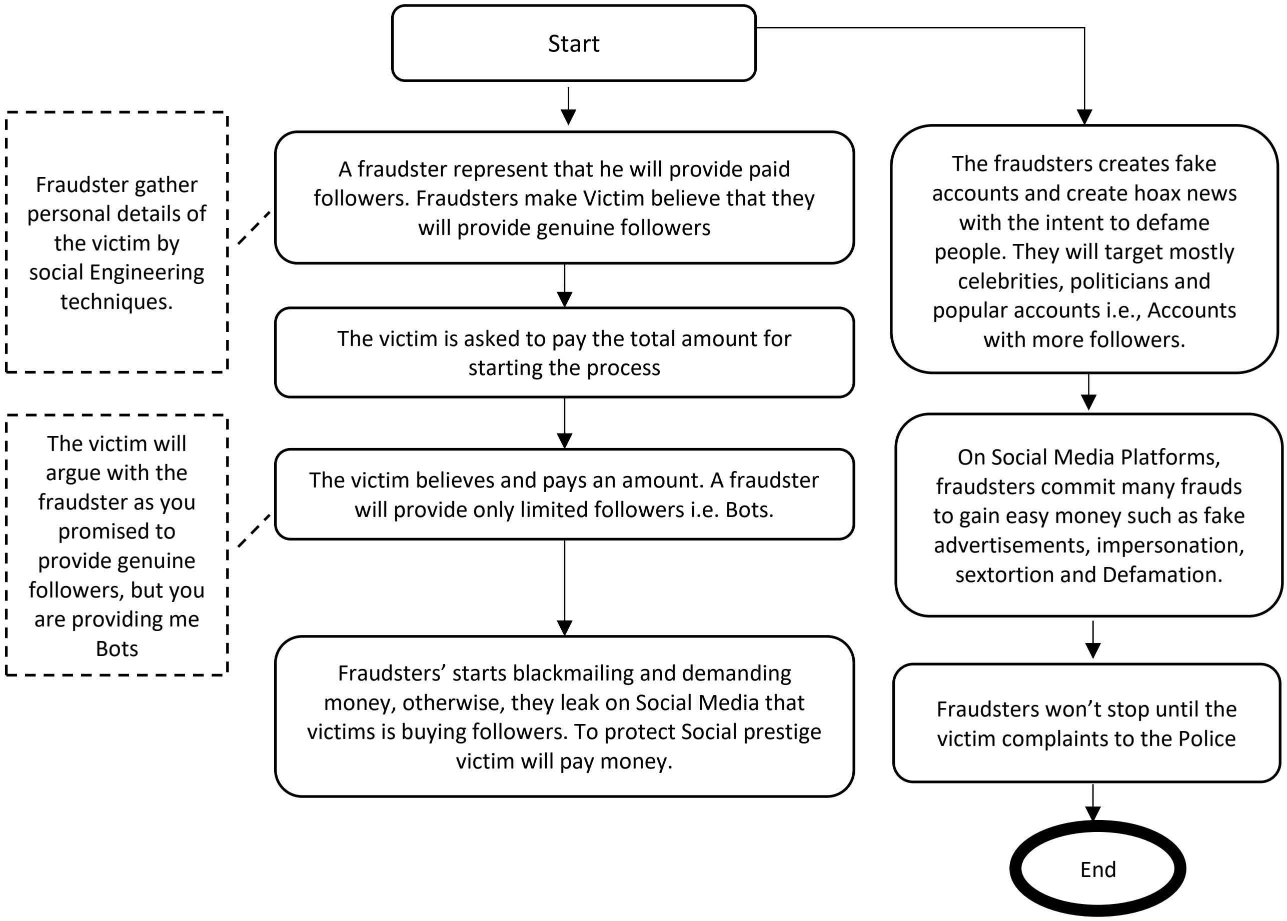
Facebook Impersonation – Fraudsters by opening fake FB accounts of victims seek money from mutual acquaintances while claiming an emergency such as hospitalization.

Honey Trapping / Cat Fishing – It's a well-known fraud in which a false social media profile is made to lure a victim and blackmail the victim for money.

Likes and Followers – In India, where bots are employed, a fraudster builds a false social media presence to sell likes, retweets, shares, comments, and followers.

Pump & dump schemes entail fraudulent and misleading claims about the market posted on social media platforms and promote a company's stock. They use social engineering techniques to get readers to buy or sell a stock swiftly before the price drops.

Social Media Fraud - Flow Chart


Start
Fraudster gather personal details of the victim by social Engineering techniques.
A fraudster represent that he will provide paid followers. Fraudsters make Victim believe that they will provide genuine followers
The victim is asked to pay the total amount for starting the process
The victim will argue with the fraudster as you promised to provide genuine followers, but you are providing me Bots
The victim believes and pays an amount. A fraudster will provide only limited followers i.e. Bots.
Fraudsters' starts blackmailing and demanding money, otherwise, they leak on Social Media that victims is buying followers. To protect Social prestige victim will pay money.
The fraudsters creates fake accounts and create hoax news with the intent to defame people. They will target mostly celebrities, politicians and popular accounts i.e., Accounts with more followers.
On Social Media Platforms, fraudsters commit many frauds to gain easy money such as fake advertisements, impersonation, sextortion and Defamation.
Fraudsters won't stop until the victim complaints to the Police
End

13.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to maintain the integrity of evidence.

The IO can collect the following evidence for investigation purposes:

- The WhatsApp chat, if applicable
- The bank account and credit card data used for transactions.
- The screenshots of UPI Transaction Details
- Call recordings between victim & fraudster, if available on the phone
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)

- Beneficiary account details
- Accused registration details on Social Media platforms such as address, Mobile Number, e-mail ID, alternate Mobile number, etc.

13.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- File a request with LEA (Law Enforcement Agency) records of Facebook / Instagram and obtain registration details and I.P. logs of the fraudster accounts.
- If the WhatsApp number is involved in fraud, serve a notice U/Sec.91 Cr. P.C, make a record request, and identify I.P. logs.
- Through IPDR, obtain the service provider, identify the ISP (Internet service provider), and send a notice U/Sec 91 Cr. P.C to the concerned ISP to get the user details.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If any website is used by the accused, find out the domain registrar from whois.domaintools.com and address a notice u/sec 91 Cr. P.C requesting to furnish the registrant details, control Panel & I.P. logs, hosting details, and payment details.
- Collect the CDR (Call Data Records) and CAF (Customer Application Form) of the suspect mobile numbers. From the CDRs, trace the suspect's locations and contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- Initiate the process of refunding of the amount to the victim.
- Trace the accused by linking the series of events

13.4 Case Study:

Nature of Offence: Social Medial Abuse

Case Details: A resident of the Medchal-Malkajgiri district submitted a petition wherein the complainant stated that she has a Facebook profile, which she has been using for two years. From the first week of July 2019, she could not open her account with her password. She knew that some people were using her account and posting obscene photos, graphic images, and videos on her Facebook wall. Fraudsters sent the above-said material to her Facebook friends, causing her agony.

In this case, IO:

1. Sent requisition to Law Enforcement Online Requests (www.facebook.com/records) for details like IP addresses during various logins to the profile, registered email address, and phone number linked to the account.
2. From the report of Facebook, IP addresses were obtained for some logins to the said profile.
3. On analysis of IP addresses for ISP details, it was found that Jio internet was used.
4. A requisition for allotment particulars of IP address was sent to Jio, and it was found that the internet of the mobile number: 6304XXXXXX was used.
5. Arrested the accused along with his mobile phone, which was used to commission this offence.
6. The mobile phone was sent to FSL for an Expert’s report.

14. ATM FRAUD

Like any systems designed to secure and disburse valuables, Automated Teller Machines (ATMs) are also prone to fraud. "ATM Fraud" is a compromise of Personal Identification Numbers (PINs) and fraudulent Debit Card use than with the coherence of ATM hardware systems.

There is also an increase in phishing attacks in ATMs. These frauds are tricked victims into giving out their PINs to the fraudsters, who used the victims' account information and PINs to create fake ATM cards and withdraw.

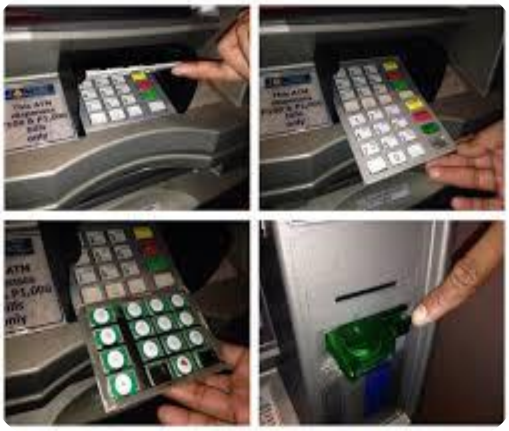
14.1 Modus Operandi:

ATM fraud and security have turn-up as significant concerns among ATM operators. Various frauds include

Shoulder Surfing

A thief makes a clone ATM card with a customer's PIN, often obtained through casual observation (shoulder surfing). The thief then takes necessary precautions to cover himself from the video surveillance and withdraws the money.

Skimmers



Criminals employ skimmer devices to collect information from the magnetic stripe on the back of an ATM card. These devices, which resemble a handheld

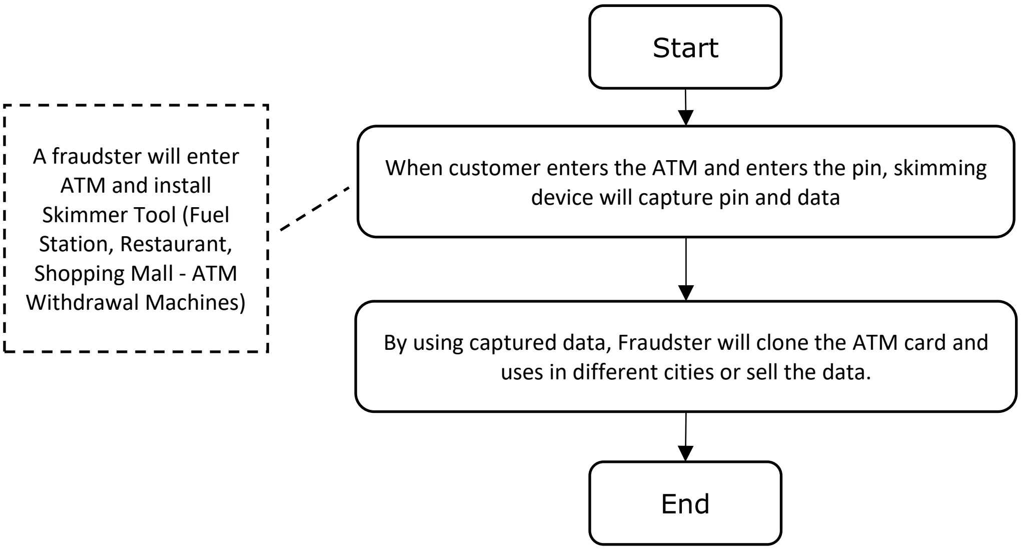
Card scanners that are commonly mounted near or on top of an ATM's card reader are smaller than a pack of cards. These gadgets are typically used to deceive customers into thinking that the skimmers are part of the ATM swiping mechanisms. When the victim inserts the card, the skimmers gather the personal information of the victim(s) who have swiped their ATM card with merchants.

Card Trapping

An ATM will dispense cash into the trap during a normal transaction. The fraudsters create a situation where the money is never presented to the customer. Thinking that the ATM has malfunctioned, the customer leaves the ATM Kiosk. Immediately, the criminal enters the facility, removes the cash trap, and takes out the cash that got stuck earlier in the dispenser. Further explaining the cash trap involves placing the adhesive tape in such a manner that blocks the cash dispenser, holds dispensed cash, and prevents cash retraction.

Jamming of Key Board: The fraudster jams essential buttons on the ATM keyboard. So that the transaction is unsuccessful, after leaving the customer from the ATM kiosk, the fraudster then enters ATM unblocks the buttons and withdraws money as the customer has already entered the details.

ATM FRAUD – FLOW CHART


Start
A fraudster will enter ATM and install Skimmer Tool (Fuel Station, Restaurant, Shopping Mall - ATM Withdrawal Machines)
When customer enters the ATM and enters the pin, skimming device will capture pin and data
By using captured data, Fraudster will clone the ATM card and uses in different cities or sell the data.
End

14.2 Expected areas of Evidence:

The IO can collect the following evidence for investigation purposes:

- CCTV footage of ATM Centre
- The details of ATM centers where money has been withdrawn
- The details of POS transactions where the cloned card is used for payments
- CCTV footage of Restaurant/ Mall where suspect/ accused skimmed the card data.

14.3 Standard Operating Procedure (SOP):

AT ATM:

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Check the bank statement of the complainant and find out where withdrawals took place. Address a letter to the bank requesting to furnish the CCTV footage of the ATM center and its surroundings.
- Find the compromised point ATM Centres if many complaints about unauthorized ATM withdrawals are filed.
- Collect the CCTV footage of the ATM center and surroundings where Card data is compromised and check if any skimmer is fixed.
- Try to find out the persons who fixed skimmers, mostly foreign nationals, involved in such frauds.
- Check if the fraudsters use any bikes/four-wheelers in the CCTV footage.

At Restaurants/shopping malls

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Check the bank statement of the complainant and find out where withdrawals took place. Address a letter to the bank requesting to furnish the CCTV footage of the ATM center.
- If any complaints about unauthorized ATM withdrawals are filed, find the compromised point (Restaurant/bar).
- After finding the compromised point find out the employees who joined recently and quit.
- Find their resumes and try to find their residential addresses.
- Find out where the withdrawals are taking place and collect the CCTV footage of the ATM Centers and surroundings.
- Trace the accused by linking the series of events

14.4 Case Study:

Mode of Violation of Law: ATM Fraud

Brief History of Offence: A complaint is received from a software employee in which he stated that he has a savings account in ICICI Bank, Hyderabad. He lost Rs. 1,00,000 from his account without his knowledge. An unknown person withdrew money from his account at Goregaon of Mumbai between 09:45 PM to 09:58 PM. Whereas during this period complainant was in Hyderabad, and the debit card was in his possession. During the investigation, it was found that similar complaints were registered against unauthorized withdrawals.

In this case, IO:

1. Collected the bank statements of the victims
2. Identified the compromised ATM centers with the help of the National payments Corporation of India (NPCI)
3. Identified withdrawal locations from bank statements & collected CCTV footage of particular ATM centers.
4. Collected CCTV Footage of ATMs, where skimmers fixed
5. Collected FRRO details of the foreigners who landed in Hyderabad during that period.
6. Based on the evidence collected, two Romania nationals were arrested when they came to withdraw the amount from ATM.
7. Sent material objects to FSL for an Expert's opinion

ജ❈ഗ

15. CYBERSTALKING / SEXTORTION

Cyber Stalking:

Cyberstalking is a form of cyberbullying. It is a crime where the stalker targets the victim with threatening/abusive messages and follows them/their activities in the real world. Criminals use the internet and other technologies to stalk a person online. Cyberstalkers usually use digital platforms like email, instant messages, phone calls, and different communication modes to stalk the victim. Cyber Stalking can be sexual harassment, inappropriate contact, unwelcome attention in a victim's life, and family activities. It may also include false accusations, posting derogatory statements, identity theft, etc.

Sextortion

Sextortion is extorting money or sexual favors from people by threatening to reveal evidence of their sexual activity.

There are various types of Sextortion.

- Sextortion through social media
- Sextortion through hacked webcams
- Sextortion through account hacking

15.1 Modus Operandi:

(a) Stalking

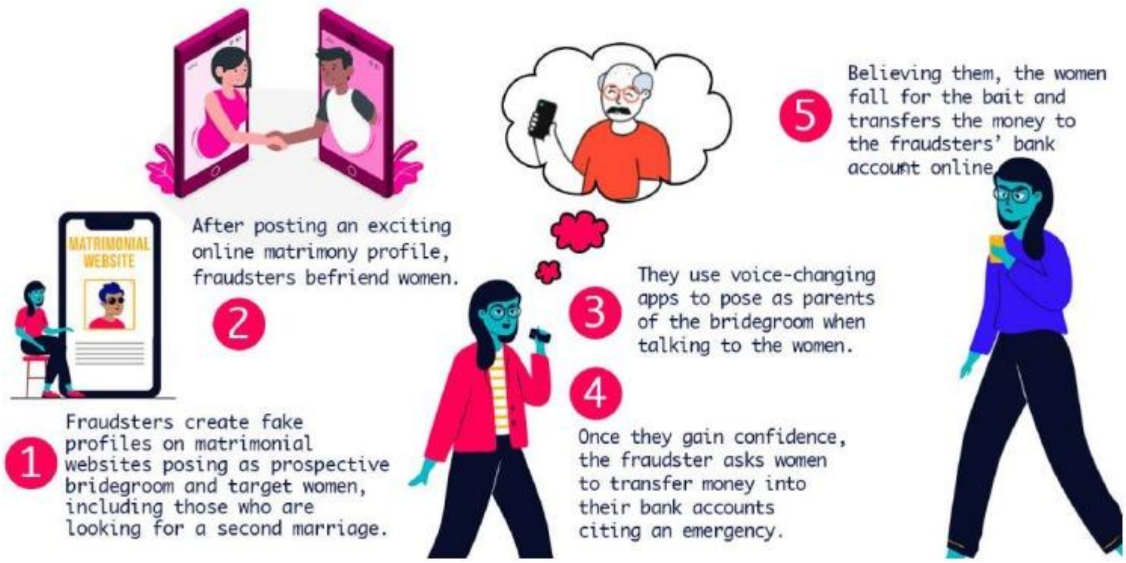
In most stalking cases, the stalker is someone the victim knows. This might be an ex-partner, a work colleague, or a rejected partner.

The stalking activity might be carried out in a current or past relationship.

- Victim uses geo-tagging (enabled location tagging) / check-in feature of social media and makes public posts on their calendar or itineraries
- The stalker keeps a watch on the victim's posts and will know about the victims' itineraries.
- Stalker uses the information and takes advantage of favourable opportunities to intimidate/ molest/ rob the victim.

i. The Stalker hacks the victim's account
ii. The Stalker gains access to the victim's contacts
iii. The stalker creates a fake profile and sends a "friend request" to the victim's contacts.

Modus Operandi



1 Fraudsters create fake profiles on matrimonial websites posing as prospective bridegroom and target women, including those who are looking for a second marriage.

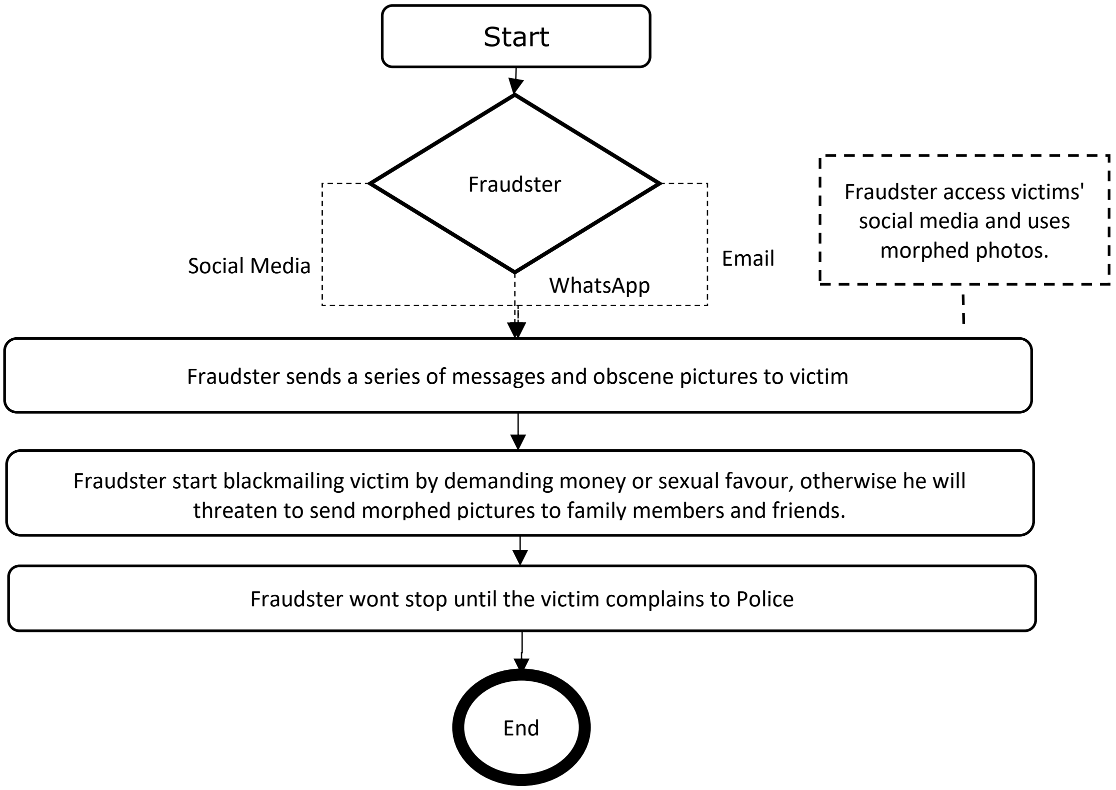
2 After posting an exciting online matrimony profile, fraudsters befriend women.

3 They use voice-changing apps to pose as parents of the bridegroom when talking to the women.

4 Once they gain confidence, the fraudster asks women to transfer money into their bank accounts citing an emergency.

5 Believing them, the women fall for the bait and transfers the money to the fraudsters' bank account online.

Cyber Stalking Fraud - Flow Chart



Fraudster access victims' social media and uses morphed photos.

Fraudster sends a series of messages and obscene pictures to victim

Fraudster start blackmailing victim by demanding money or sexual favour, otherwise he will threaten to send morphed pictures to family members and friends.

Fraudster wont stop until the victim complains to Police

(b) Sextortion

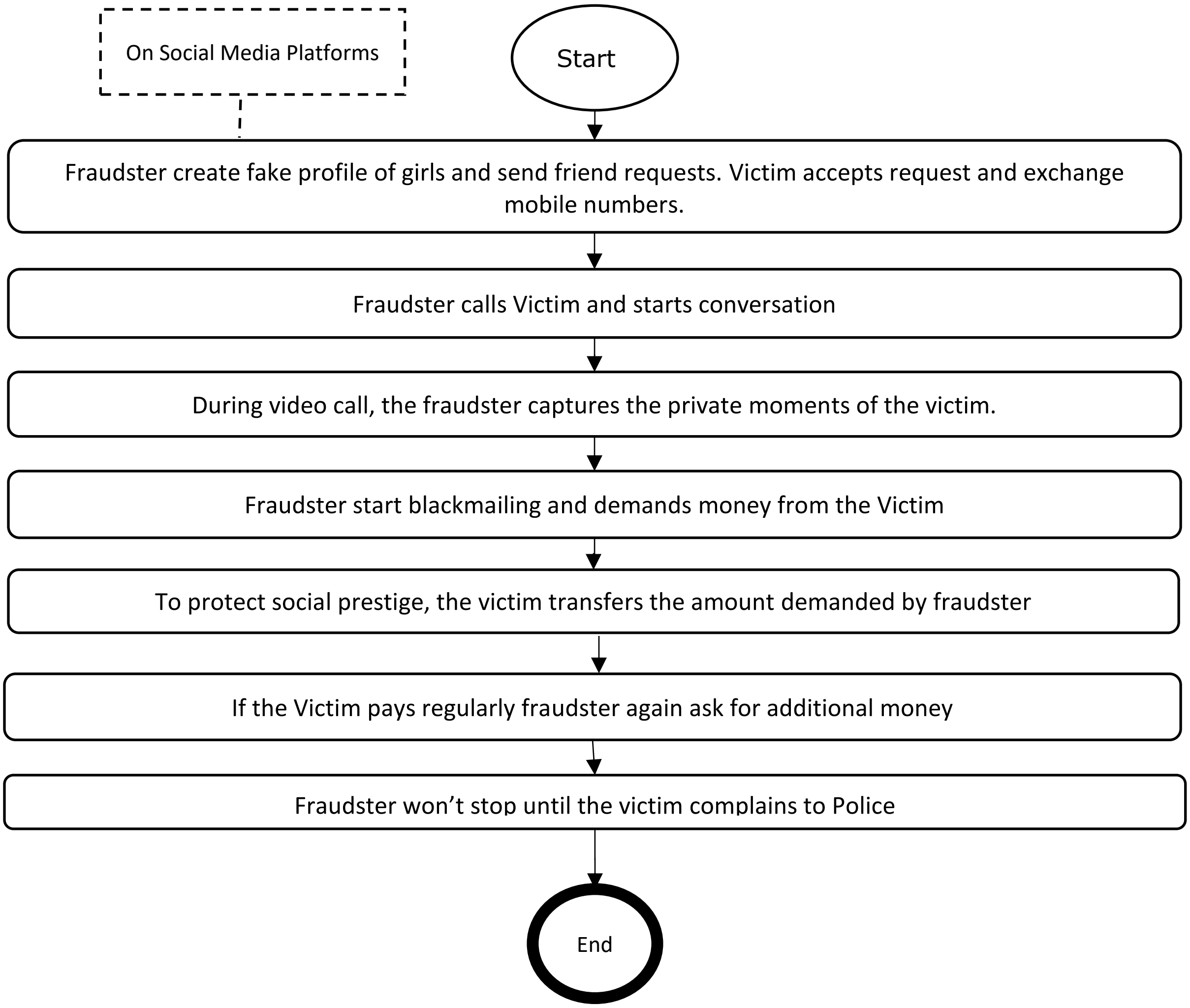
- Criminals pretend to be young women/men on dating apps and gather victims' personal information.
- Once the targets are identified, they lure them with photos and invite them for real-time video chats
- Criminals express strong emotions too fast and suggest getting nude in a video call
- The offender will then record the entire activities
- The criminal will then threaten the victim that those videos will be published if they don’t pay money
- Blackmailing often continues even after the victim pays the money

15.2 Expected areas of Evidence

The IO can collect the following evidence for investigation purposes:

- Social media usernames, e-mail IDs, phone No of Suspect/ accused
- Service Providers collect the details of IP addresses, registered mobile numbers, etc.
- CAF/SDR/CDR/IPDR of the accused phone number.
- KYC documents and IMEI numbers
- The beneficiary account details
- The details of financial transactions
- Screenshots of messages
- Last know location of the suspect/ accused

Sextortion – Flow Chart


On Social Media Platforms
Start
Fraudster create fake profile of girls and send friend requests. Victim accepts request and exchange mobile numbers.
Fraudster calls Victim and starts conversation
During video call, the fraudster captures the private moments of the victim.
Fraudster start blackmailing and demands money from the Victim
To protect social prestige, the victim transfers the amount demanded by fraudster
If the Victim pays regularly fraudster again ask for additional money
Fraudster won’t stop until the victim complains to Police
End

15.3 Expected Areas of Evidence:

The investigating officer/Cyber Warrior has to collect the following information for investigation purposes:

- Personal Details of the victim include name, Phone number, and address.
- Details of the social media profile page of the fraudster
- Screenshots of the messages/content
- Recordings of phone calls (if any)
- User Registration details of the accused. (Email ID, Alternate email ID, Mobile No., Date of Creation, etc.)
- Last Known locations of the suspect/ accused
- Beneficiary account details.

15.4 Standard Operating Procedure (SOP):

Cyber Stalking/ Sextortion:

- Prepare a plan of action for the case
- Identify the bullying platform and send a notice U/Sec 91 Cr. P.C requesting to furnish the registration details and mobile number of the suspect/ accused.
- Collect the CDRs of suspect mobile numbers. If the suspect number is toll-free, identify the service provider and request connection details and CDRs.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- If any other services available are found, serve notice u/sec 91 Cr. P.C and collect the registration details, mobile numbers, email IDs, etc.
- Trace the accused by linking the series of events

15.5 Case Study:

Mode of Violation of Law: Cyber Stalking/ Sextortion.

Case Details: A female tennis player lodged a complaint stating that she received abusive and threatening messages on her Viber account. Further, the stalker created an imposter Instagram account to defame her integrity. The accused met her by stating that he had a plan to participate in Para Olympics and requested the complainant to share a diet plan. Initially, the complainant did it, and later accused started harassing her to marry. He constantly abused using indecent and foul language. He contacted her from different mobile numbers and used the Viber application to threaten her. The accused impersonated the victim's Instagram account and chatted with her friends in the victim's name to defame her integrity.

In this case, IO:

1. Collected the registration details of fake Instagram account ID, Viber ID, and accused Mobile details from Service Providers
2. Collected CDR, SDR details of accused Mobile number and identified the location
3. Collected IP logs from the Service Provider
4. Based on IP location, the accused was traced.
5. Sent material objects to FSL for an Expert's opinion

ꕥ

16. SOCIAL MEDIA IMPERSONATION FRAUD

Social media impersonation is digital identity theft. It is one of the most common crimes happening these days. Impersonation is where a fraudster creates social media accounts mimicking a legitimate account. Impersonators pretend to be like friends or family members to orchestrate a highly targeted social engineering attack. Some imitate professionals like recruiters, lawyers, politicians, film personalities, activists, IT agents, or popular company/brand representatives. A simple search on any search engine can give criminals all the information they need to build a fake account; profile picture, description, interests, and activities. Each attack leaves behind a trail of digital breadcrumbs that can be followed to predict when and where future attacks will be carried out.

TYPES OF IMPERSONATORS:

Bot: These are fake public accounts that try to imitate the actual user and post similar stuff. The number of followers is small, and they follow a lot of other accounts that are similar to theirs. No full name, no biography, and no profile photographs are some of the traits.

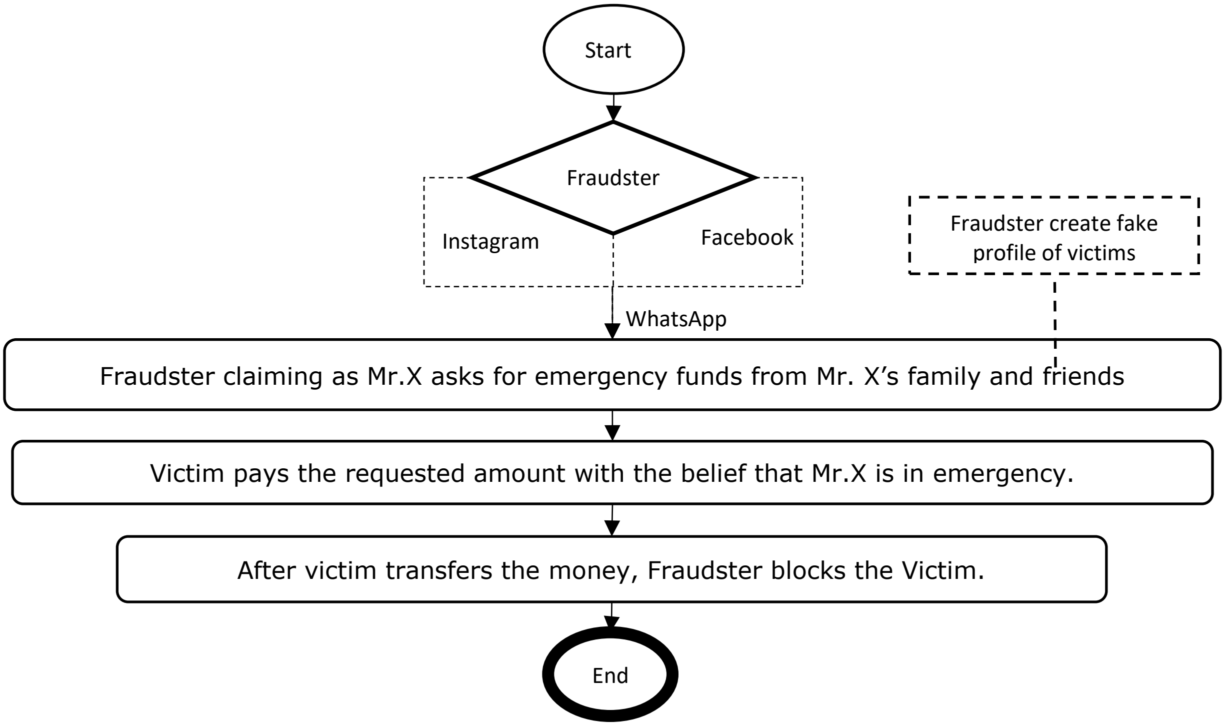
Crime: An imposter attempts to impersonate another person or brand to commit fraud, such as obtaining confidential information or acquiring access to property that is not theirs.

Entertainment: An entertainer impersonates a celebrity for amusement and makes fun of their personal lives.

16.1 Modus Operandi:

Fraudsters create phony accounts on prominent social media platforms like Facebook and Instagram. They send a message to the victim’s acquaintance, requesting money for urgent medical needs, payments, etc. Fraudsters can also establish trust over time and utilize personal information for extortion or blackmail. Fraudsters may also exploit victims' personal information to impersonate victims on the internet, thereby putting victims at risk.

Impersonation Fraud - Flow Chart


Start
Fraudster
Instagram
Facebook
WhatsApp
Fraudster create fake profile of victims
Fraudster claiming as Mr.X asks for emergency funds from Mr. X's family and friends
Victim pays the requested amount with the belief that Mr.X is in emergency.
After victim transfers the money, Fraudster blocks the Victim.
End

16.2 Expected areas of evidence:

The IO can collect the following evidence for investigation purposes:

- Social Media ID details of fraudster
- Registration details of the accused on Social Media
- Fraudster's Mobile Number & e-mail ID
- Beneficiary account details
- Screenshots of financial transactions

16.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- File a request with LEA (Law Enforcement Agency) records of Facebook /Instagram and obtain registration details and I.P. logs of the fraudster accounts.
- If the WhatsApp number is involved in fraud, serve a notice U/Sec.91 Cr. P.C, make a record request, and identify I.P. logs.
- Through IPDR, obtain the service provider, identify the ISP (Internet service provider), and send a notice U/Sec 91 Cr. P.C to the concerned ISP to get the user details.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts.

- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- Collect the CDR (Call Data Records) and CAF (Customer Application Form) of the suspect's mobile numbers. From the CDRs, trace the suspect's locations his contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Trace the accused by linking the series of events

16.4 Case Study:

Nature of Offence: Impersonation Fraud

Case Details: The complainant stated that she has a Facebook profile; it did not open when she tried to open it. She thought it was due to a technical issue/internet problem. Later, after a few days, a Facebook friend asked her what had happened to her and why she had been in the hospital a few days ago. She was shocked and informed that she was well and at home. Then, her friend told the complainant that someone had messaged her from the complainant's Facebook account and asked for money for the hospital bill. After that, many of her friends contacted her and informed her of the same matter, then, she came to know that someone had hacked her Facebook account, and the accused was asking for money from her friends/family members.

In this case, IO**:**

1. Sent a requisition to Law Enforcement Online Requests (www.facebook.com/records) for details like IP addresses during various logins to the profile, registered email address, and phone number linked to the account.
2. From the report of Facebook, IP addresses were obtained for some logins to the said profile. On analysis of IP addresses for ISP details, it was found that Jio internet was used.
3. Sent a requisition for obtaining particulars of IP address to TSPs and got the culprit's addresses
4. Arrested the accused persons along with material objects
5. Material objects were sent to FSL for experts' opinion

17. INSURANCE FRAUD

Insurance frauds have increased a lot during the Covid-19 pandemic. Insurance frauds are generally committed in the health care industry, automotive industry, and other insurance-related areas.

There are two types of insurance frauds – hard frauds & soft frauds. Hard frauds include when someone purposefully plots or invents a loss, such as stealing the car or setting fire to a property covered by an insurance policy. Soft frauds or opportunities include policyholders exaggerating valid claims.

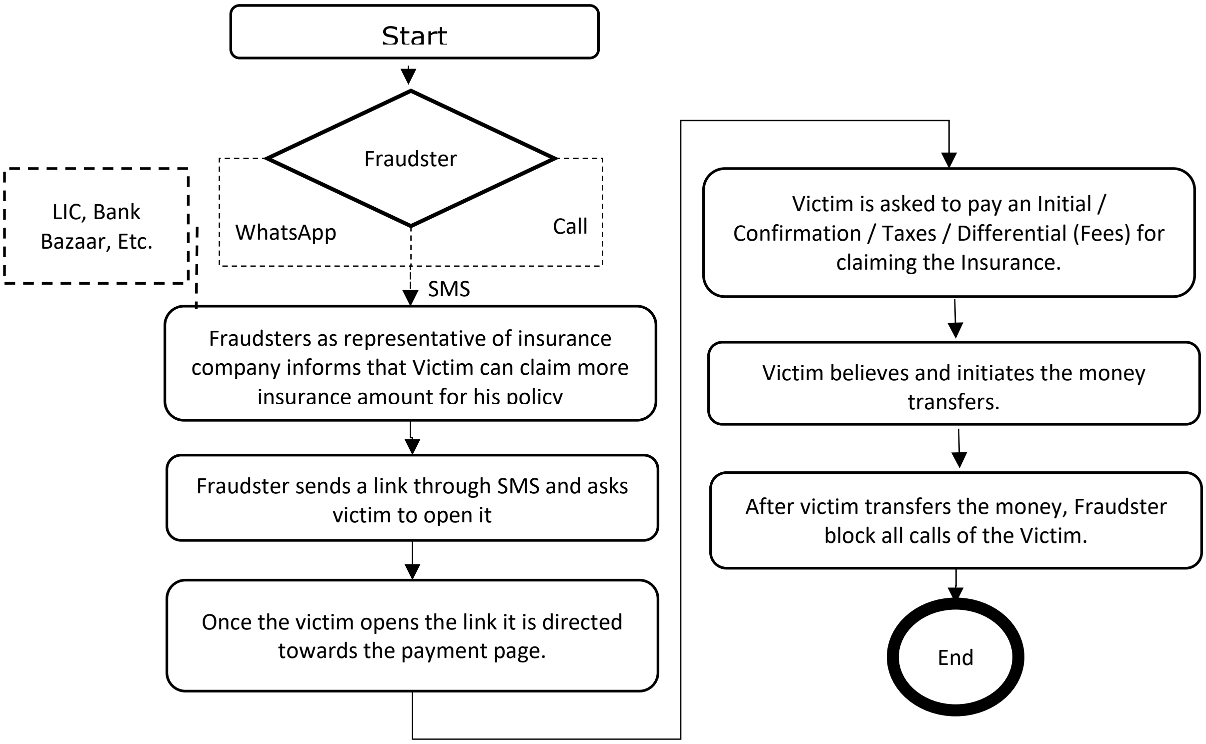
For the last few years, the number of fraud cases has increased. Insurance fraud happens when a person or a group of people tries to make money by either not complying with the terms and conditions of the insurance agreement or by discovering ways to exploit loopholes in the terms and conditions of the insurance agreement. Insurance agents, prospective policyholders, claimants, and, in some cases, staff are all involved in perpetuating these frauds.

17.1 Modus Operandi:

A few scenarios of Insurance frauds brought to the notice of companies, regulators and whistle-blowers are:

- Producing forged documents
- Non-disclosure of critical information
- Buying policies in the name of a dead person or a person with a terminal illness
- Stating false reasons for claims
- Misappropriation of assets
- Inflating expenses
- Manipulating pre-policy health check-up records
- Staged accidents and fake disability claims

Insurance Fraud - Flow Chart


Start
Fraudster
LIC, Bank Bazaar, Etc.
WhatsApp
Call
SMS
Fraudsters as representative of insurance company informs that Victim can claim more insurance amount for his policy
Fraudster sends a link through SMS and asks victim to open it
Once the victim opens the link it is directed towards the payment page.
Victim is asked to pay an Initial / Confirmation / Taxes / Differential (Fees) for claiming the Insurance.
Victim believes and initiates the money transfers.
After victim transfers the money, Fraudster block all calls of the Victim.
End

17.2 Expected Areas of Evidence:

The Investigating Officer has to understand the modus operandi and likely activity related to the crime to know the expected areas of evidence to be collected for further investigation. Enough care may be taken while collecting digital evidence by following the crime scene protocols and chain of custody to maintain the integrity of evidence.

The IO can collect the following evidence for investigation purposes:

- The WhatsApp chat and social media account details
- The bank account and credit card data used for transactions.
- The insurance policy details with the company(LIC, Bajaj, etc.)
- The Screenshots of the Payment Application and its connected numbers (Both Victim and Culprit)
- The names and titles used by the fraudsters.
- The details of messages and emails.
- Open the victim’s account, collect screenshots of the fraud transactions
- In Bank Statement – Highlight the concerned transactions for further analysis and easy corroborations.
- The beneficiary account details

- The call recordings between accused and victim, if available on the mobile phone

17.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- If a fraudster makes customers avail of new insurances, then identify the broking/insurance company in the bonds.
- Analyze the victim's bank statement and find the beneficiary accounts.
- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If the complainant received any BULK SMS in the name of Insurance money, then collect the sender of Bulk SMS Ex: QP-ICICLE from the following link https://www.findandtrace.com/trace-bulk-sms-sender
- Identify the service provider and serve a notice U/sec 91 Cr. P.C to collect the user details, KYC documents, etc.
- If the complainant received any mails, serve a notice U/Sec 91 Cr. P.C to the mail service provider and collect registration details, recovery mail ID, mobile number I.P. logs, etc.
- Check the mail source or header to find whether mail is routed through the proper channel. If the mail ID is routed through a fake mail service, address a mail to a fake service provider and collect the original I.P. logs.
- If any sites are involved, find out the domain registrar from whois.domaintools.com and address a notice u/sec 91 Cr. P.C requesting to furnish the registrant details, control Panel & I.P. logs, hosting details, and payment details.
- Send a request to the Service Provider to deactivate the Mobile number of the accused so that the same number is not used for committing crimes.
- Collect the Call Data Records (CDR) of the suspect mobile numbers from which calls were received and linked to the bank account & mail-ID. From the CDRs, trace the suspect's location his contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspect mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if

available), Truecaller (for identifying name and suspect image if available) applications.

- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- Initiate the process of refunding the amount to the victim.
- Trace the accused by linking the series of events

17.4 Case Study:

Nature of offence: Insurance fraud

Case details: Complainant stated that in June-2015, he received a phone call from an unknown caller in which he was told Rs.18,12,642/- was approved on his insurance policy. Rs.10,77,200/- is approved for the insurance fund, and Rs.7,35,442/- is approved for shareholding. After that accused informed the complainant to claim the insurance amount of Rs.18,12,642/-. The complainant needs to make two life insurance policies for a tax benefit in the name of the Exide life insurance for Rs.1,25,000/- and Rs.99,999/-. Believing the same, the complainant gave one cheque for Rs.1,25,000/- in the name of Exide Life Insurance by cheque No.054214 of SBH Hyderabad, Rs.99,999/- Cheque of IDBI Bank of Hyderabad. After paying the amount, the complainant received two Exide Life Insurance Policies. Later the complainant received another call wherein he was told that his insurance amount was increased to Rs.28,68,000/- and asked him to deposit Rs.2,11,000/- for tax. Again complainant deposited Rs.2,11,000/- in Panjab National Bank through RTGS. Again the complainant received a call from cell no.965456XXXX. The fraudster acting as an Income Tax Officer told him that his amount of Rs.28,99,000/- had been released, and the complainant needed to pay Rs.2,37,448/- for income tax. The complainant paid Rs.2,37,448/- through RTGS in Punjab National Bank. Later he realized that this was all fraud, and the above-said persons cheated him.

In this case, IO**:**

1. Sent Notices to the concerned banks with a request to furnish the statement and address particulars of the account numbers in which the complainant deposited the money.
2. Froze all the bank accounts of the accused
3. Obtained the call data of the Mobile numbers involved in this case and analyzed call data and the tower locations
4. Based on the tower locations, arrested the accused and recovered three laptops, 11 hard discs, and 29 cell phones.
5. Sent Laptops, hard disks and cell phones to FSL for Expert’s opinion.

18. ADVERTISEMENT FRAUD

Advertisement fraud is an attempt to defraud digital advertising networks for financial gain. The Indian digital advertising ecosystem currently outnumbers most other countries in volume and growth. Furthermore, the increased availability of smartphones and internet services has allowed businesses to communicate directly with their customers via mobile devices.

Any attempt to deceive digital advertising networks for financial benefit is ad fraud. Fraudsters frequently utilize bots to commit ad fraud. They use a variety of strategies to trick advertisers and ad networks into paying them.

18.1 Modus Operandi:

Cybercriminals use a variety of ways to carry out ad fraud. Some of the methods include:

a. **Click Hijacking:** When an attacker redirects a click on one ad to a second ad, the click is effectively stolen. To carry out this fraud, the attacker must gain access to the user's computer, the website of the ad publisher, or a proxy server.

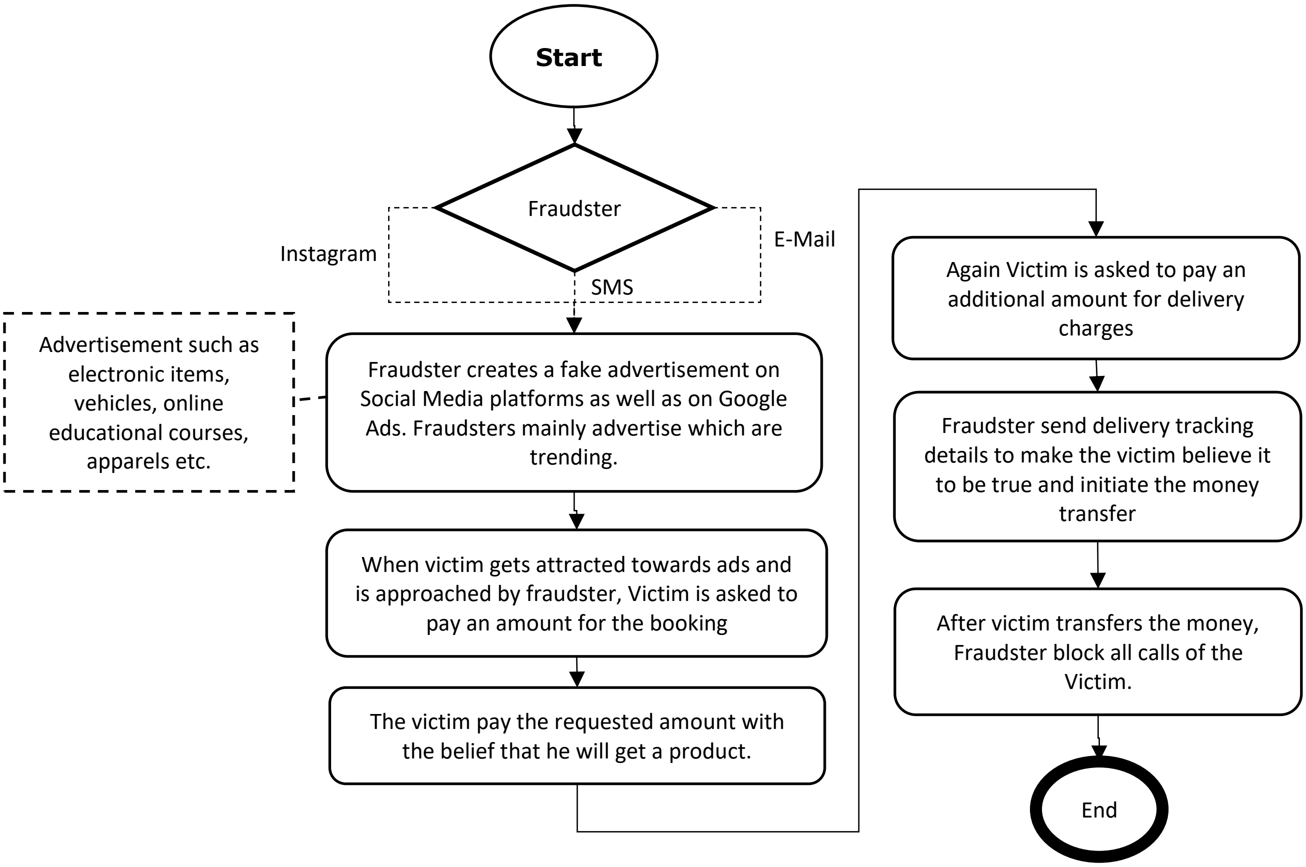
b. **Fake App Installation:** Ads are frequently displayed within mobile apps. For this type of fraud, fraudsters employ groups of people to install apps thousands of times.

c. **Botnet Ad Fraud:** Fraudsters can use botnets to generate thousands of fake clicks on an ad or fake visits to a website displaying the ads.

d. **Hidden Ads:** This fraud targets ad networks that pay based on impressions (views), not clicks.

Platforms like OLX and Quikr are being used to target the victims and cheat them on the pretext of making a deal

ADVERTISEMENT FRAUD - FLOW CHART


Start
Fraudster
Instagram
SMS
E-Mail
Advertisement such as electronic items, vehicles, online educational courses, apparels etc.
Fraudster creates a fake advertisement on Social Media platforms as well as on Google Ads. Fraudsters mainly advertise which are trending.
When victim gets attracted towards ads and is approached by fraudster, Victim is asked to pay an amount for the booking
The victim pay the requested amount with the belief that he will get a product.
Again Victim is asked to pay an additional amount for delivery charges
Fraudster send delivery tracking details to make the victim believe it to be true and initiate the money transfer
After victim transfers the money, Fraudster block all calls of the Victim.
End

18.2 <u>Expected area of evidence:</u>

The IO can collect the following evidence for investigation purposes:

- Screenshots of social media chat details
- Social Media registration details of the accused
- Contact details of the suspect/ accused, e.g., Mobile Number, Email ID, Social Media IDs &, etc.
- CDR, SDR, IMEI, and KYC particulars of accused
- Screenshots of financial transactions
- Beneficiary account details

18.3 Standard Operating Procedure (SOP):

- Prepare a plan of action for the case
- While visiting the scene of the crime, carry a checklist form
- Address a letter to the platform u/Sec 91 Cr. P.C is requesting to furnish the user details who posted the advertisement.

- If amounts are transferred to bank accounts, collect transaction statements, Account Opening Form, PAN Number, Email ID, and Mobile number linked to the bank account of beneficiary accounts. Subsequently, obtain CCTV Footage, UPI transaction details, IMPS & RTGS transaction details.
- Find if the funds are further transferred to other accounts. If so, collect the details of the other accounts involved.
- If the fraudster duped the victim by sending a Q.R. code, it is concluded that the fraudster holds a merchant account. In such case, serve notice U/Sec 91 Cr. P.C to the wallet and collect Photos, pictures of the store/shop, Geolocation, ID proofs, and Bank account.
- Collect the CDRs& CAFs of the mobile numbers from which calls are received. From the CDRs, trace the suspect's locations his contacts. From the messages received on the mobile number, trace the banks, websites, or any other services availed by the suspect.
- Search the suspected mobile numbers in open-source tools such as Eyecon (to identify Eyecon image, WhatsApp image, Facebook account if available), Truecaller (for identifying name and suspect image if available) applications.
- Subsequently, search suspect numbers in UPI/e-Wallet applications (Identify the name, bank details & UPI ID if available).
- Initiate the process of refunding the amount to the victim.
- Trace the accused by linking the series of events

19. REPORT A CYBERCRIME

How to utilise the national cyber-crime portal:

- The Ministry of Home Affairs (MHA) has set up a dedicated platform for reporting cyber-crimes from anywhere. Though it caters to all types of cyber-crimes, it emphasizes cyber-crimes against women and children. Once a complaint is filed on this portal, it is forwarded to the relevant law enforcement agency nearest to the complainant. The Ministry of Home Affairs (MHA) has also started a helpline with 1930 number, which functions 24x7.
- A victim can file the complaint both online and offline, and the victim can choose as per his/her convenience. The cyber-crime complaints can be registered with the designated cyber crime police stations at all three Police Commissionerate - Rachakonda, Cyberabad & Hyderabad.

  National cyber-crime reporting portal :

  - (a) Register at https://cybercrime.gov.in/ (You will be required to use register via OTP from a valid Indian number)
  - (b) Choose the Category and Sub-Category of the Complaint

    i. **Report Women/ Child related Crime –**

    a) Report & Track / Report Anonymously
       - Child Pornography (CP) – Child Sexual Abuse Material (CSAM)
       - Rape/Gang Rape (RGR)-Sexually Abusive Content
       - Publishing or Transmitting Sexually Obscene material in electronic form

    ii. **Report Other Cyber Crimes –**

    a) Online and Social Media Related Crime
    b) Online Financial Fraud
    c) Hacking/Damage to computer, Computer system, etc.
    d) Online Cyber Trafficking
    e) Online Gambling
    f) Ransomware
    g) Cryptocurrency Crime
    h) Cyber Terrorism
    i) Any Other Cyber Crime

  - **Incident:**

    (a) Mode of Communication (Internet, WhatsApp etc.)
    (b) Date & Time
    (c) Platform (Internet, WhatsApp etc.)

(d) Upload Evidence (Screenshots of Payments / Bank Statement's for financial frauds.

For Harassment or any other attach related, Screenshots, Pictures, Audio, Video, etc.

- **Suspect Details (If Available):**
  (a) Suspect Name
  (b) Identity (Mobile, Email, etc.)
  (c) Location (Workplace etc.)
- **Complainant's Details:**
  (a) Full Name & Supporting Details (Father, Spouse, Guardian etc.)
  (b) Email ID / Phone Number
  (c) Address & ID Proof (Aadhar etc.)

Detailed step by step procedure to file a complaint:

- Report Crime related to Women or Children – https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportCPRGRcomplaints-v10.pdf
- Report other Cyber Crimes – https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

Important points to remember:

- Victims can file a complaint at the nearest Cyber Crime Police Station for a quicker response
- Victims can also file a complaint on the Online Cyber Crime Portal Anonymously without giving their identity; the entire complaining process remains the same, just that victims don't disclose themselves.

20. CITIZEN FINANCIAL CYBER FRAUD REPORTING & MANAGEMENT SYSTEM (CFCFRMS)

The Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) has been developed in-house by I4C to integrate Law Enforcement Agencies, Banks, and Financial Intermediaries. It is currently being utilized with **1930** (earlier 155260) number, which functions 24x7.

The facility empowers the banks and the police by leveraging new-age technologies to share online fraud-related information and take action in almost real-time. The loss of defrauded money in online cheating cases can be stopped by chasing the money trail and stopping its further flow before the fraudster takes it out of the digital ecosystem. The facility empowers the banks and the police, sharing online fraud-related information and taking action in almost real-time.

Step by Step Process of Complaint:-

- Victims can call on Helpline no. **1930**, manned and operated by the respective State Police officers.
- The Cyber Police notes down the fraud transaction details (Account Number, Wallet, UPI, Transaction ID, Date, Debit/Credit Card Numbers Etc) and other basic personal information of the caller and submits a Ticket on the portal
- The Ticket gets escalated to the concerned Banks, Wallets, Merchants, and so on, depending on whether they are the victim’s bank or the bank/wallet in which the defrauded money has gone.
- An SMS is also sent to the victim with an acknowledgment number of the complaint with directions to submit complete details of the fraud on the portal within 24 hours using the acknowledgment number.
- The concerned Bank, which can now see the ticket on its dashboard on the Reporting Portal, checks the details in its internal systems.
- If the victim’s money is still available, the Bank puts it on hold, i.e., the fraudster cannot withdraw the money. If the victim’s money has moved out to another Bank, the Ticket gets escalated to the next subsequent Bank to which the money has moved out. This process is repeated until the money is saved from the hands of the fraudsters.

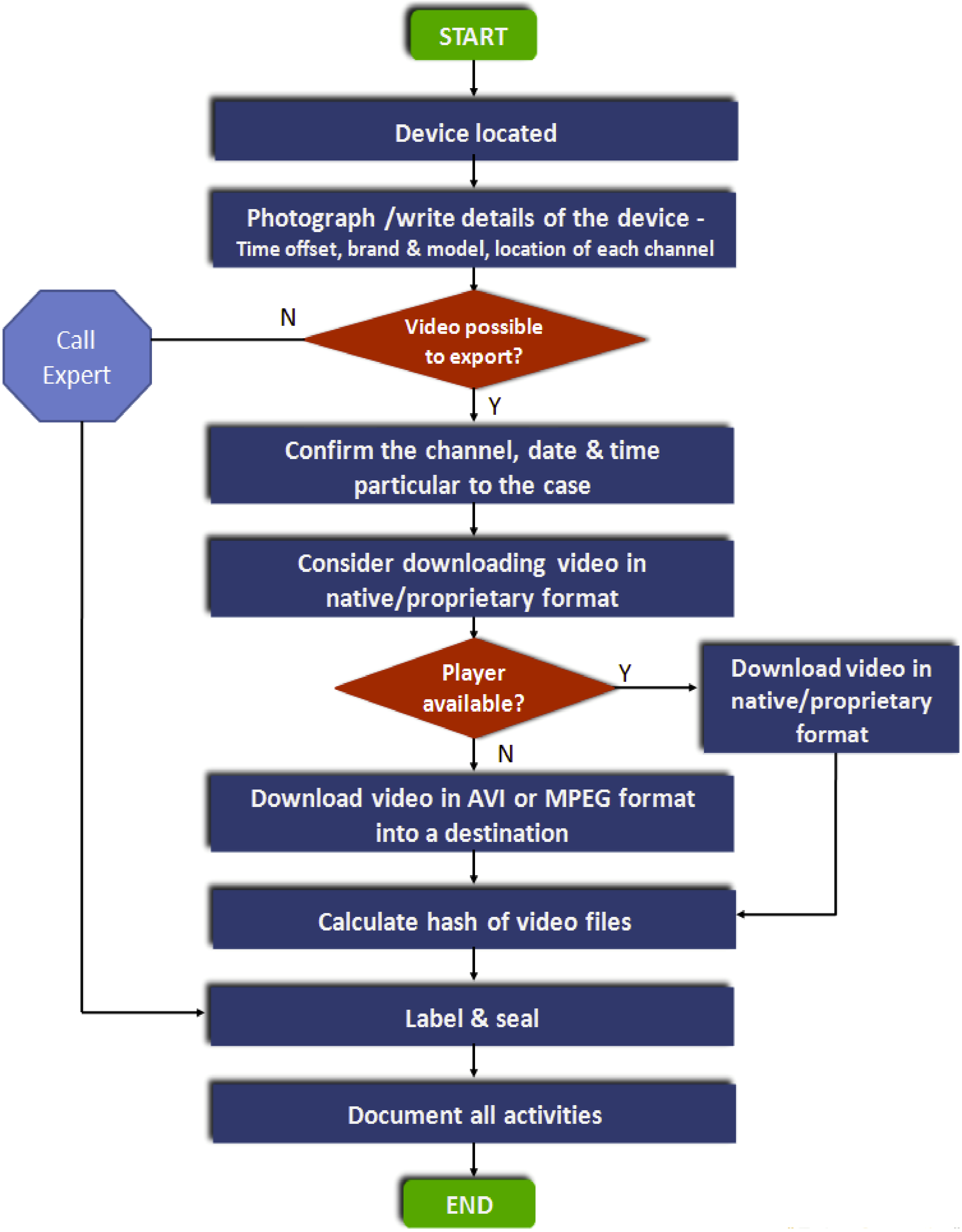
References:

1. https://www.facebook.com/cybercrimepolice.gov.in
2. https://cybercrime.gov.in/
3. https://www.infosecawareness.in/
4. http://isea.gov.in/
5. https://cert-in.org.in/
6. https://staysafeonline.org/
7. https://cytrain.ncrb.gov.in/
8. https://vikaspedia.in/e-governance/citizen-services/citizen-financial-cyber-fraud-reporting-and-management-system

21. IMPORTANT POINTS

Points to be noted while collecting CCTV/DVR Systems:

- DVR make, model and number
- Whether DVR is PC-based or Standalone, or Networked
- No. of cameras having input support
- No. of recording units installed
- No. of Active and Inactive cameras
- Camera Make and Model
- Note, whether the camera is IR sensitive
- System date and time
- Actual date and time
- Correlation between System and actual date and time
- Recording capacity of the System and method of overwriting
- System Password
- System settings
- Quality of recording, i.e., high, medium, low
- Frames/pictures per second
- Frame size
- Details of HDDs. - Make, Model, S/N, Capacity
- System Firmware version
- Event logs.
- Playback software name and version.
- Whether any recent backup of the recordings available?
- Details of any incident of importance, its date and time details.
- Details of Camera Positions.
- Details of native/proprietary file formats the system uses for storing the recordings.


START
Device located
Photograph /write details of the device -
Time offset, brand & model, location of each channel
Video possible to export?
N
Call Expert
Y
Confirm the channel, date & time particular to the case
Consider downloading video in native/proprietary format
Player available?
Y
Download video in native/proprietary format
N
Download video in AVI or MPEG format into a destination
Calculate hash of video files
Label & seal
Document all activities
END

Flow Chart for seizure and retrieval of video footage from CCTV/DVR systems

Scientific Approach To Investigation

1. Prepare a Plan of Action
2. Prepare a rough sketch of the scene
3. Always carry a check-list at the Scene of Crime (SOC)
4. Maintain neutrality of thinking/ No preconceived notion
5. Follow the Grid method for searching the Crime scene
6. Maintain proper chain of custody
7. Collating/Corroborating pieces of evidence
8. Linking Accused to Scene of Crime (SOC)
9. Connecting pieces of evidence to SOC
10. Identify resources, both internal & external, for investigation
11. Prepare a Flow Chart of the investigation
12. Prepare a calendar of evidence (Oral and documentary)
13. Evidence to be collected in chronological order/ event wise
14. Send material objects to FSL for expert's opinion
15. Collect evidence from all angles (i.e., 360°)

The Evidence in The System/Device

1. Date & Time of the system
2. Check the Start menu to know the frequent activities of the user
3. Take a screenshot of files & folders available on the desktop
4. Check the change programme or uninstall option in 'This PC' to understand the types of software installed
5. Check for encrypted software (like True crypt)
6. Find Hidden files and folders
7. Check changes in file extensions to know Extension mismatch, if any
8. Check Recycle bin, temporary folder, downloads folder for deletions and downloads to understand the user activity
9. In-Browser check for History, Passwords, Bookmarks, add-ons, etc.
10. Find IP address & MAC address (ipconfig/all)
11. Check System information
12. Collect the details of the displayed WIFI connections
13. Check the Google activity of the user to know the search history
14. Device movement – Android phone synced to Google

Evidence From WhatsApp

1. Chat details
2. Profile details
3. Group descriptions
4. Details of invite links
5. Deleted images/files
6. User common groups
7. Details of blocked contacts
8. Chat group member details
9. WhatsApp Call logs (Audio/Video)
10. Stickers
11. Voice notes
12. Backup details
13. Status messages
14. Shared media files
15. WhatsApp version
16. Documents details
17. WhatsApp web sessions
18. WhatsApp payment details

Evidence From Android Phone

1. Passwords
2. Deleted files
3. Geo-location
4. Contact details
5. Calendar entries
6. Bank credentials
7. Credit/ Debit card details
8. Photos
9. Text messages
10. Internet Cookies
11. Downloaded documents
12. Internet browsing history
13. Downloaded applications
14. Call logs (Dialled/ Received)

Dozen Cs of Investigation

1. **Crime Registration** – Entering facts in Relevant Registers & Systems
2. **Crime Scene Visit** & Evaluation, Draw Rough Sketch of Scene
3. **Crux of the case** understanding – Preparing Plan of Action
4. **Collecting Evidence** –DOC (Documentary, Oral, Circumstantial)
5. **Correlation among Evidence** – Remove counterproductive evidence
6. **Chain of Custody** – Maintaining Integrity of Evidence
7. **Connecting** Accused & Evidence to Scene of Crime (SOC)
8. **Confirm & Corroborate Evidence** - Witnesses & Experts
9. **Complete missing points** & Review the Evidence, if any (Oral & Documentary)
10. **Charge Sheet** the case - prepare a flow-chart of evidence
11. **Court proceedings** – Briefing Witnesses & Prosecutor on key points
12. **Case disposal** – Conviction/Acquittal

Chain of Custody

Chain of custody, in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence.

Chain of custody is essential for evidence documentation. It includes:

- When is evidence obtained?
- Who obtained the evidence?
- Who secured the evidence?
- Where does the evidence come from?
- Where is it stored?

The chain of custody is established whenever an investigator takes custody of evidence at a crime scene. The chain of custody helps to authenticate the evidence by preventing tampering. If the chain of custody is broken, evidence could become legally worthless. Collection, preservation, packaging, transportation, storage, and creation of the inventory list are all part of the chain of custody process.

Section 65-B of the Indian Evidence Act: Admissibility of electronic record. This section makes the electronic evidence admissible in the form of computer output (printout) or the data copied on electronic or magnetic media.

Important judgements related to Section 65-B of IEA:

1. Paras Jain Vs. State of Rajasthan
2. Shafi Mohammed Vs. State of Himachal Pradesh
3. P.V. Anwar Vs. P.K. Basheer

Crime Scene Evaluation – Search & Seizure of Digital Evidence:

- Reaching the crime scene as soon as possible (ASAP) with a tool kit & checklist
- 'As is where is' documentation
- Take Photos and Video of the crime scene covering all angles
- When System is ON - take a photo of the screen
- Collect - printouts, chits, scribble notes, etc.
- In case of perishable data, take a photograph and document it
- Network Identification such as Network devices- modem, router
- Collect peripherals and take latent fingerprints
- Note Passwords found on walls, tables, notebook
- Take the hash value of digital evidence
- Record the location of all cables of the system
- Note - make, model, and serial number of system/device
- Collect software manual/written documentation from scene
- Protect digital evidence from electromagnetic sources
- Use antistatic bags for storing digital evidence
- Document everything is done at the crime scene
- Ensure proper chain of custody
- Don't alter the condition of electronic devices
- Don't allow the accused/suspect to handle digital evidence
- Don't turn the computer ON; if it is OFF
- Don't allow the computer to shut down normally
- Proper labeling, packing, and transportation of objects
- Don't use plastic bags for storing digital evidence
- Mouses, keyboards, and monitors do not contain digital evidence
- Always follow the standard operating procedures while seizing digital evidence

Charge Sheet Preparation:

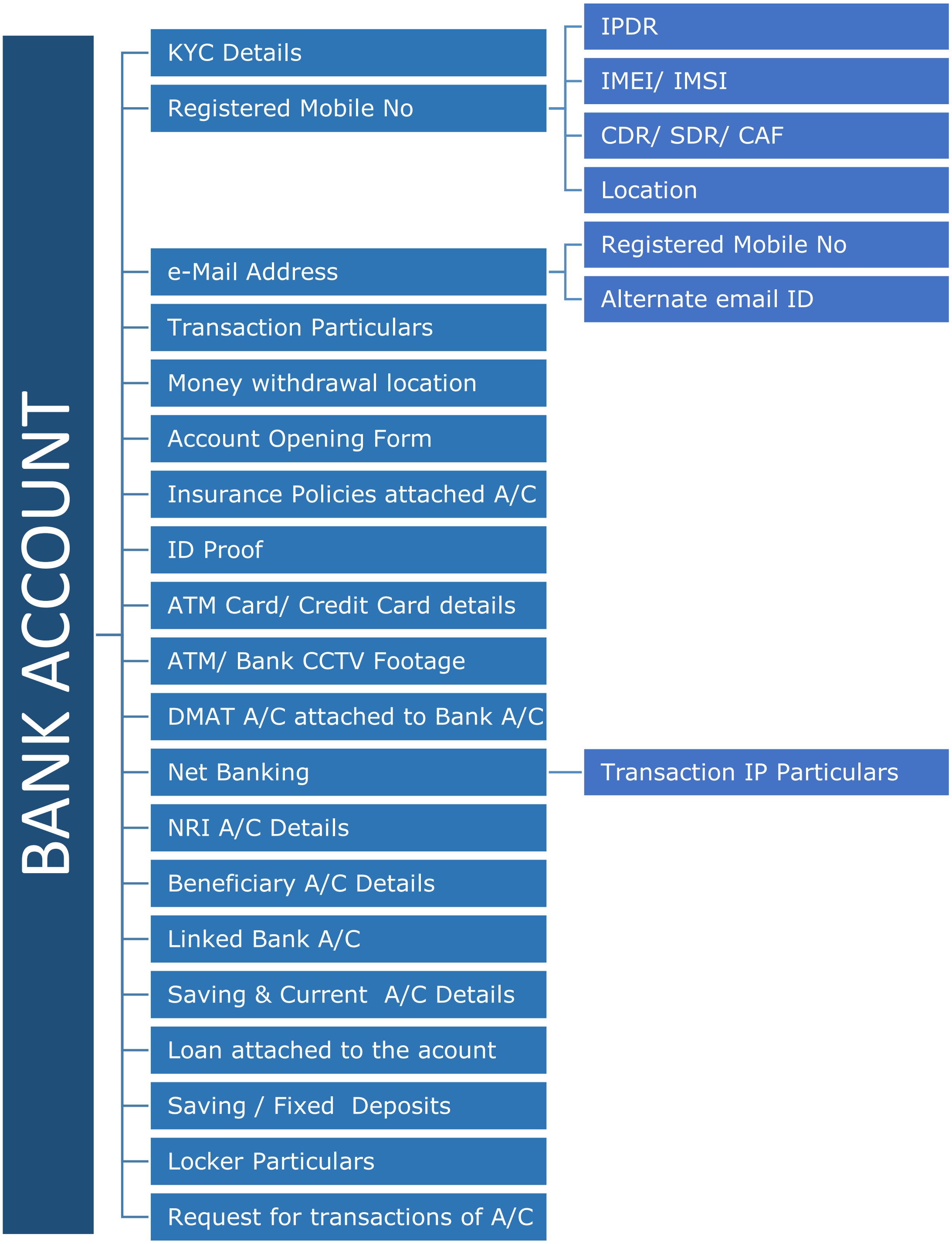
Drafting of charge sheet is vital in securing a conviction in the case. A systematic framing of a charge sheet detailing all the procedures followed in collecting the evidence, maintaining the chain of custody, and details of the Expert's opinion will strengthen the prosecution case and improves the chances of conviction of the accused/adjudication of the case. The following should be incorporated into the Charge Sheet.

1. FIR contents and evidence obtained during the investigation are to be incorporated into the charge sheet
2. Mention crime scene details, search and seizure procedure, and chain of custody
3. Mention drawing of rough sketch of the scene, FSL report

4. Corroborate the collected evidence with the section of law registration in the case
5. If the ingredients of some other section of law are attracted during the investigation, file a requisition in honourable court for the addition of sections or as the case may be for deletion or alteration of the charges.
6. Substantiate the section of law with the oral evidence
7. Present the evidence in chronological order or event-wise
8. The witness statements should include that they can identify the documents seized and explain their relevance to the case
9. Discuss the technicalities involved in the case in simple terms
10. Discuss what evidence has been collected against each of the accused about each of the alleged offences
11. Check whether all information contained in the charge sheet is supported by evidence (oral, circumstantial, or documentary) gathered during the investigation. If not, identify the gaps and collect the necessary information
12. Please ensure that accused numbers and witness numbers assigned to the persons are maintained throughout the body of the charge sheet correctly
13. If applicable, mention previous convictions & previous crime history of the accused in the charge sheet. Attach relevant documents
14. Mention whether any LOC or Red Corner Notice was issued during the investigation
15. Mention whether any statements U/s 164 Cr.P.C. were recorded
16. Always draw a flow-chart of evidence and attach it to the charge sheet for easy understanding of the public prosecutor and the judge (Also useful for IO during deposition of evidence in honourable court)
17. Mention at the end, if any further investigation is to be carried out.
18. Check whether the list of witnesses, list of documents, and list of material objects are enclosed
19. Prepare a calender of evidence (Oral and documentary)
20. Collect the medical certificates and other documents. Mention the source of the said documents and the manner of collection of the said documents (like from witness/ using 91 CrPC, etc.)
21. In critical cases, take the opinion/approval of the public prosecutor before filing the charge sheet.

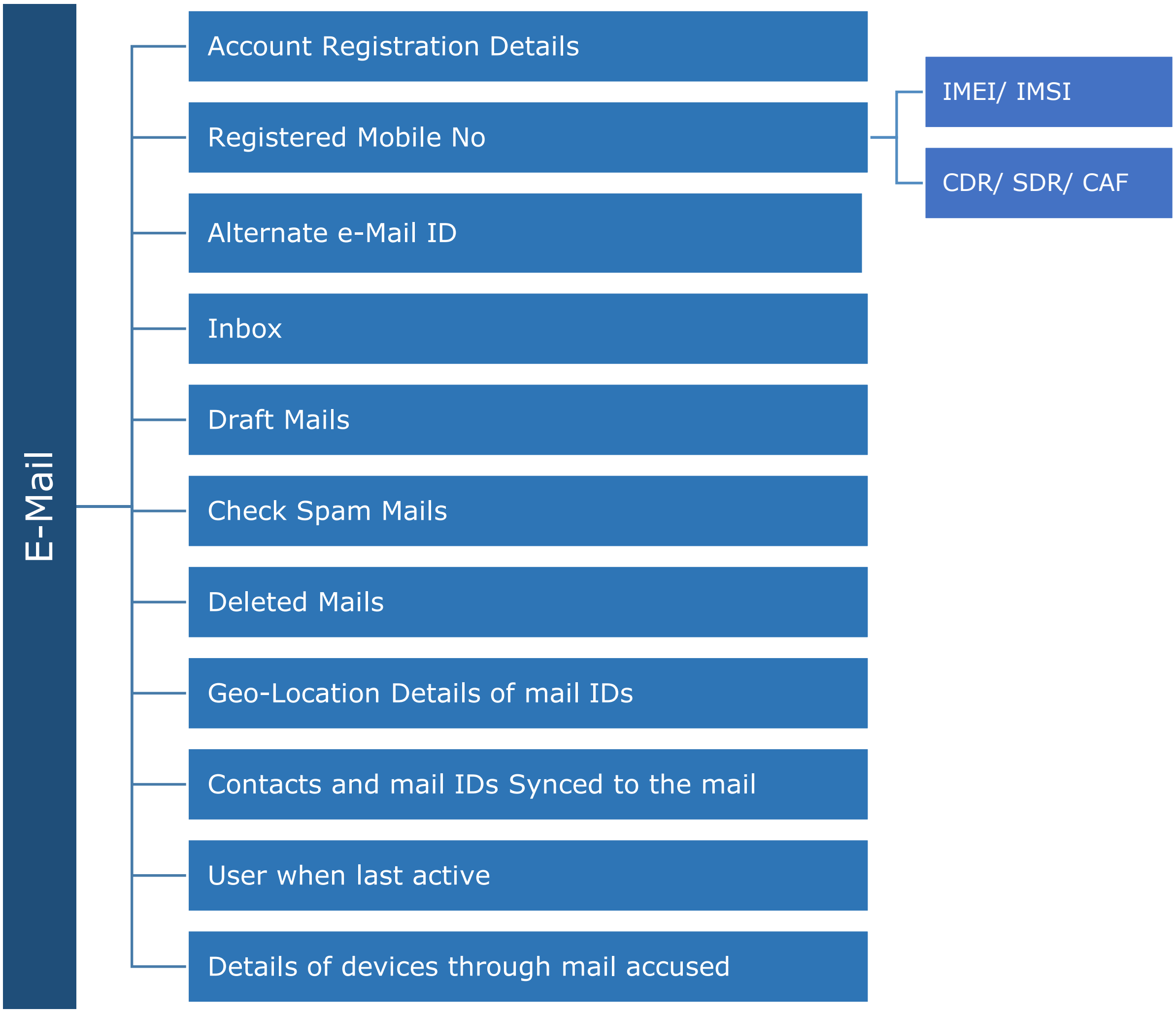
22. WORKFLOW CHARTS

Bank/ Financial Institution



- BANK ACCOUNT
  - KYC Details
  - Registered Mobile No
    - IPDR
    - IMEI/ IMSI
    - CDR/ SDR/ CAF
    - Location
  - e-Mail Address
    - Registered Mobile No
    - Alternate email ID
  - Transaction Particulars
  - Money withdrawal location
  - Account Opening Form
  - Insurance Policies attached A/C
  - ID Proof
  - ATM Card/ Credit Card details
  - ATM/ Bank CCTV Footage
  - DMAT A/C attached to Bank A/C
  - Net Banking
    - Transaction IP Particulars
  - NRI A/C Details
  - Beneficiary A/C Details
  - Linked Bank A/C
  - Saving & Current A/C Details
  - Loan attached to the acount
  - Saving / Fixed Deposits
  - Locker Particulars
  - Request for transactions of A/C

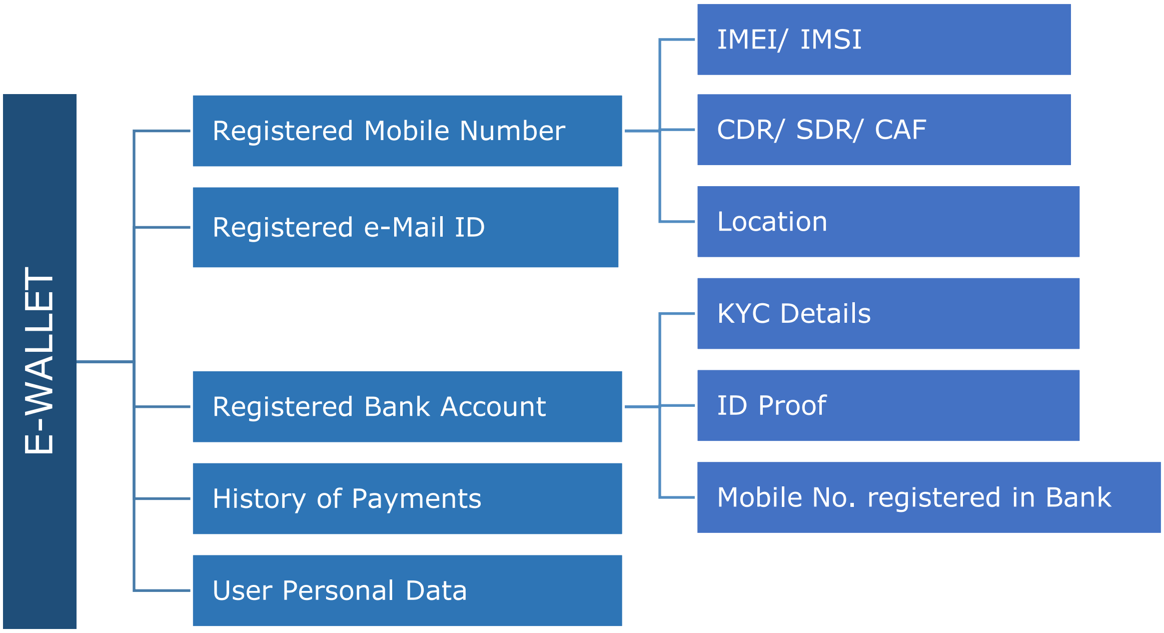
E-Mail Investigation



E-Mail

- Account Registration Details
- Registered Mobile No
  - IMEI/ IMSI
  - CDR/ SDR/ CAF
- Alternate e-Mail ID
- Inbox
- Draft Mails
- Check Spam Mails
- Deleted Mails
- Geo-Location Details of mail IDs
- Contacts and mail IDs Synced to the mail
- User when last active
- Details of devices through mail accused

E-Wallet Investigation



E-WALLET

Registered Mobile Number

- IMEI/ IMSI
- CDR/ SDR/ CAF
- Location

Registered e-Mail ID

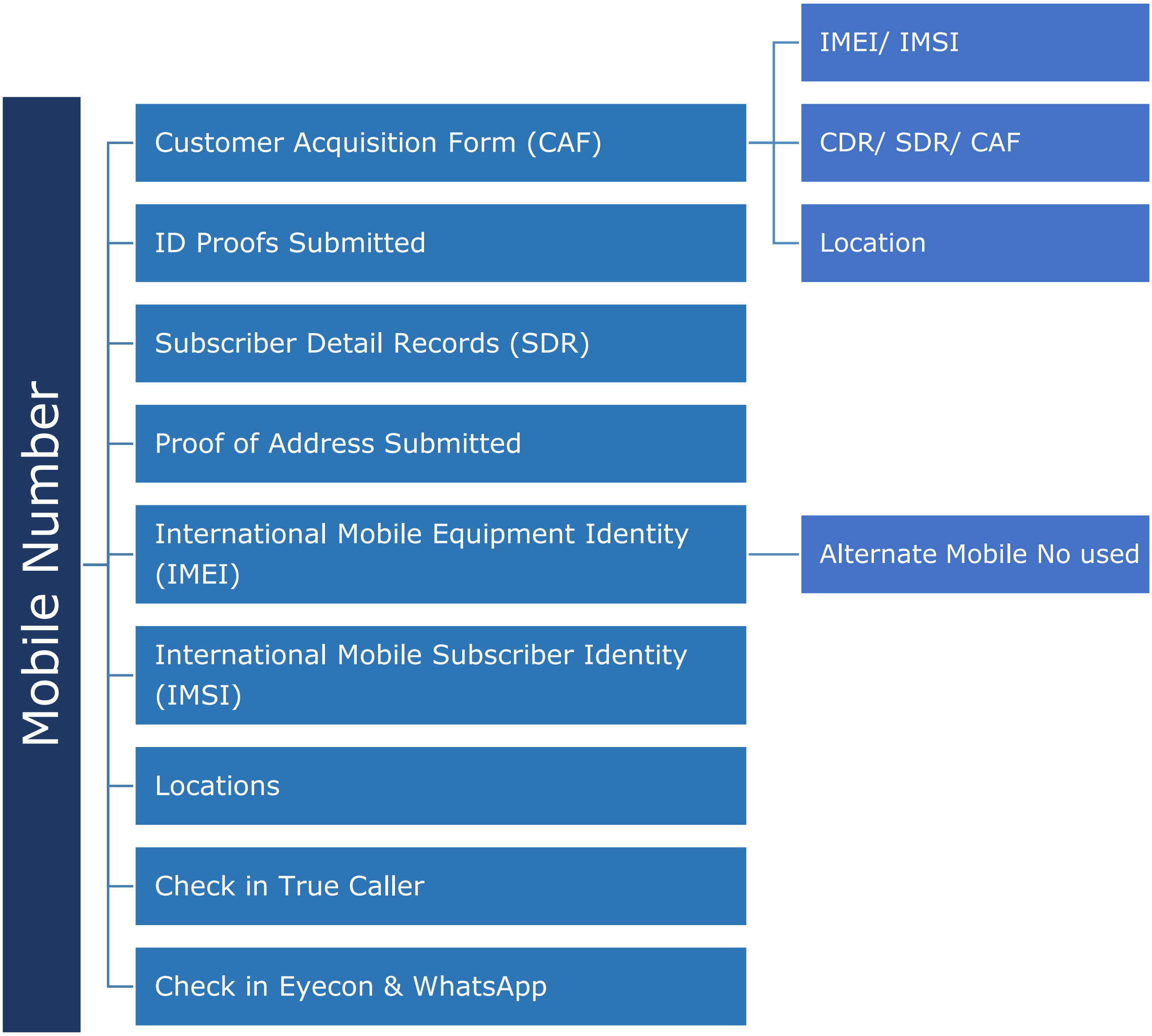
Registered Bank Account

- KYC Details
- ID Proof
- Mobile No. registered in Bank

History of Payments

User Personal Data

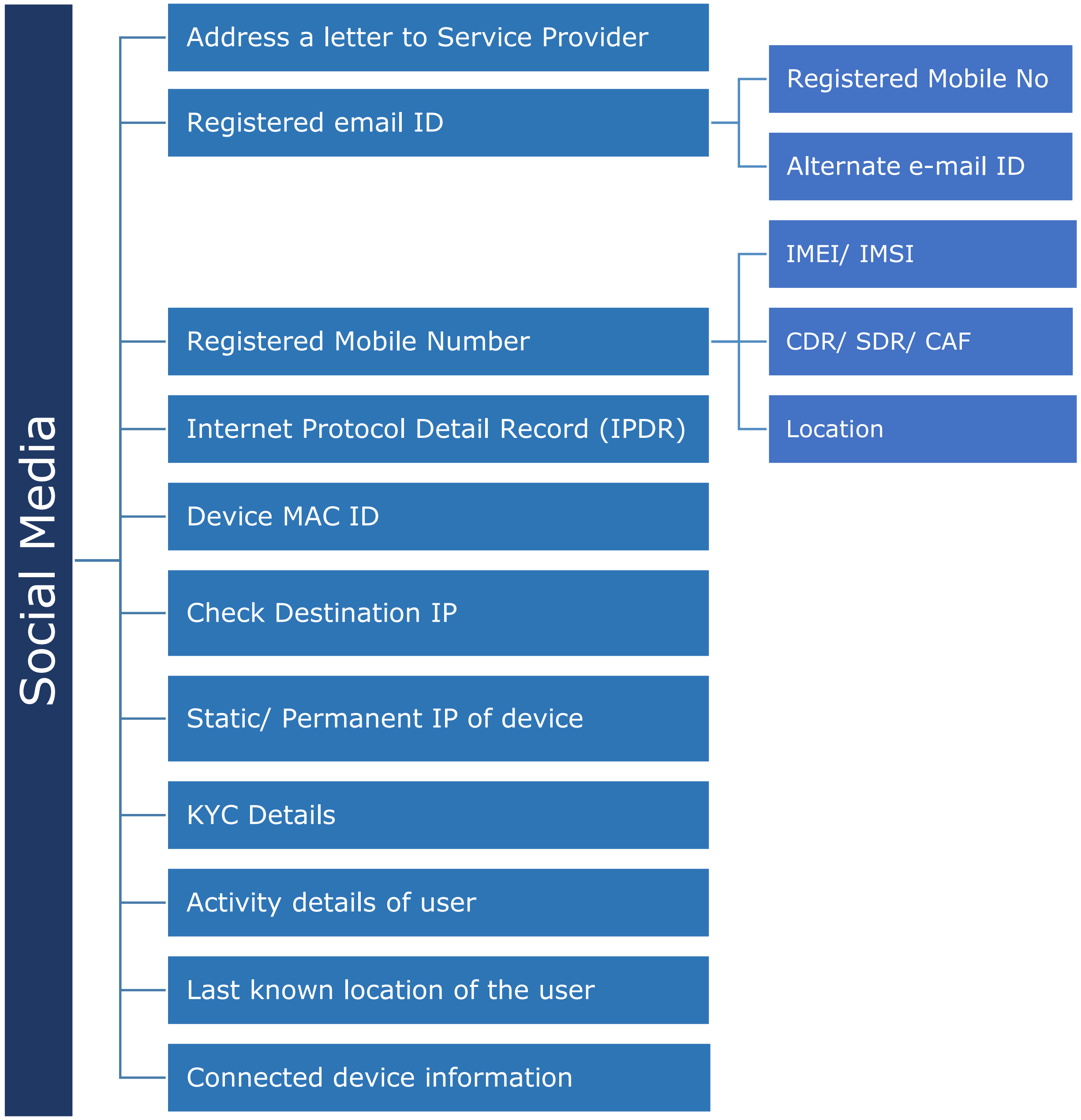
Mobile Number Investigation



Mobile Number

- Customer Acquisition Form (CAF)
  - IMEI/ IMSI
  - CDR/ SDR/ CAF
  - Location
- ID Proofs Submitted
- Subscriber Detail Records (SDR)
- Proof of Address Submitted
- International Mobile Equipment Identity (IMEI)
  - Alternate Mobile No used
- International Mobile Subscriber Identity (IMSI)
- Locations
- Check in True Caller
- Check in Eyecon & WhatsApp

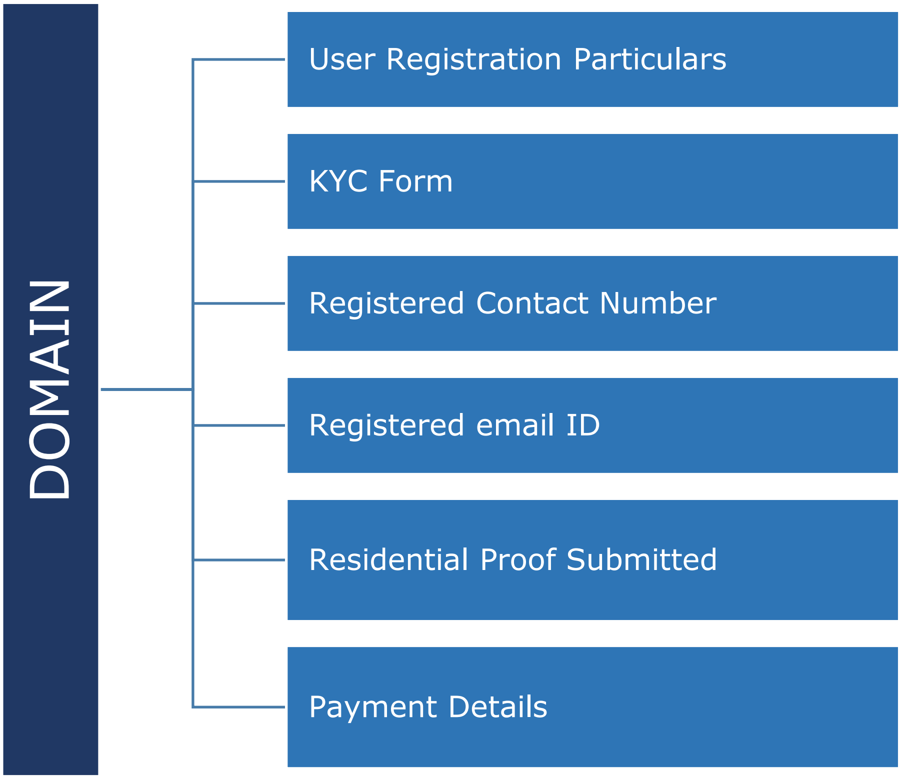
Social Media Fraud



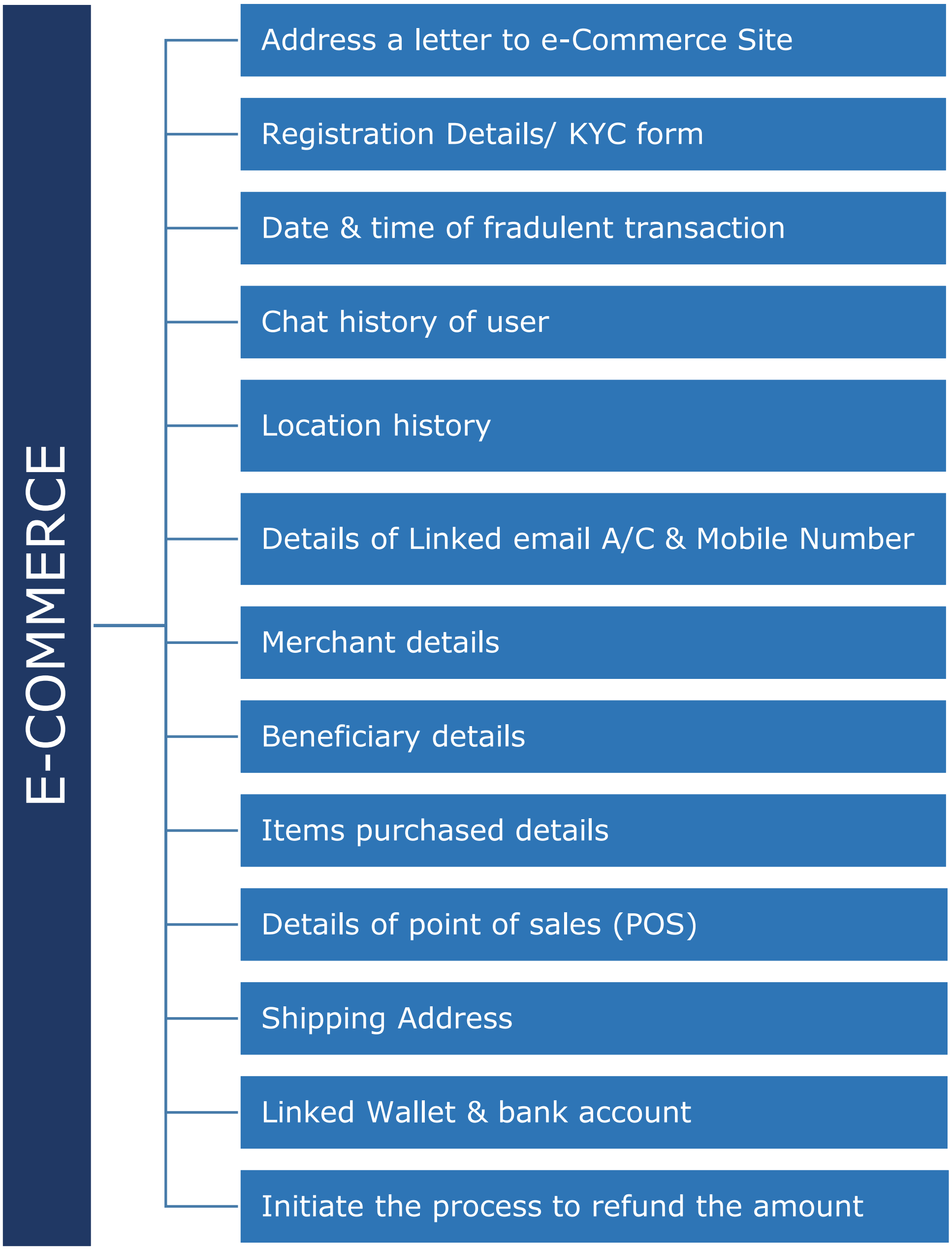
Social Media

- Address a letter to Service Provider
- Registered email ID
  - Registered Mobile No
  - Alternate e-mail ID
- Registered Mobile Number
  - IMEI/ IMSI
  - CDR/ SDR/ CAF
  - Location
- Internet Protocol Detail Record (IPDR)
- Device MAC ID
- Check Destination IP
- Static/ Permanent IP of device
- KYC Details
- Activity details of user
- Last known location of the user
- Connected device information

Domain


DOMAIN
User Registration Particulars
KYC Form
Registered Contact Number
Registered email ID
Residential Proof Submitted
Payment Details

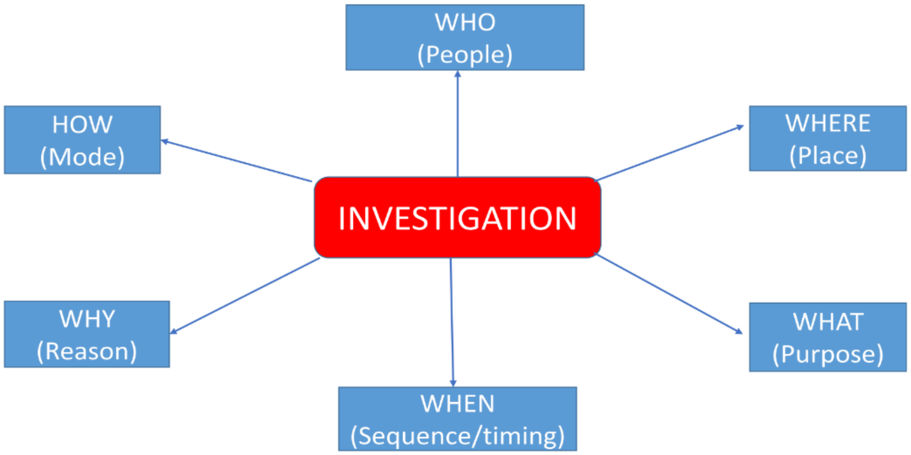
E-Commerce Fraud



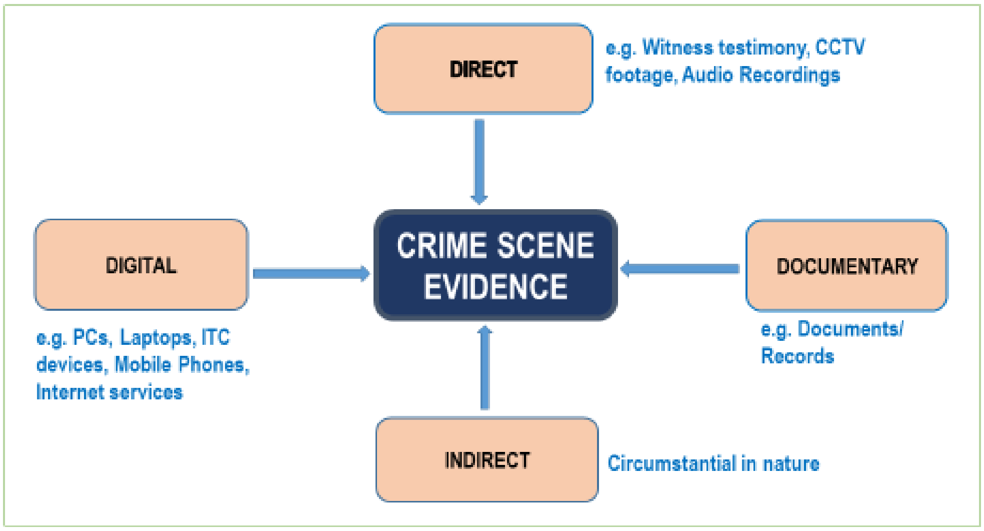
E-COMMERCE

- Address a letter to e-Commerce Site
- Registration Details/ KYC form
- Date & time of fradulent transaction
- Chat history of user
- Location history
- Details of Linked email A/C & Mobile Number
- Merchant details
- Beneficiary details
- Items purchased details
- Details of point of sales (POS)
- Shipping Address
- Linked Wallet & bank account
- Initiate the process to refund the amount

5 Ws & 1 H OF INVESTIGATION



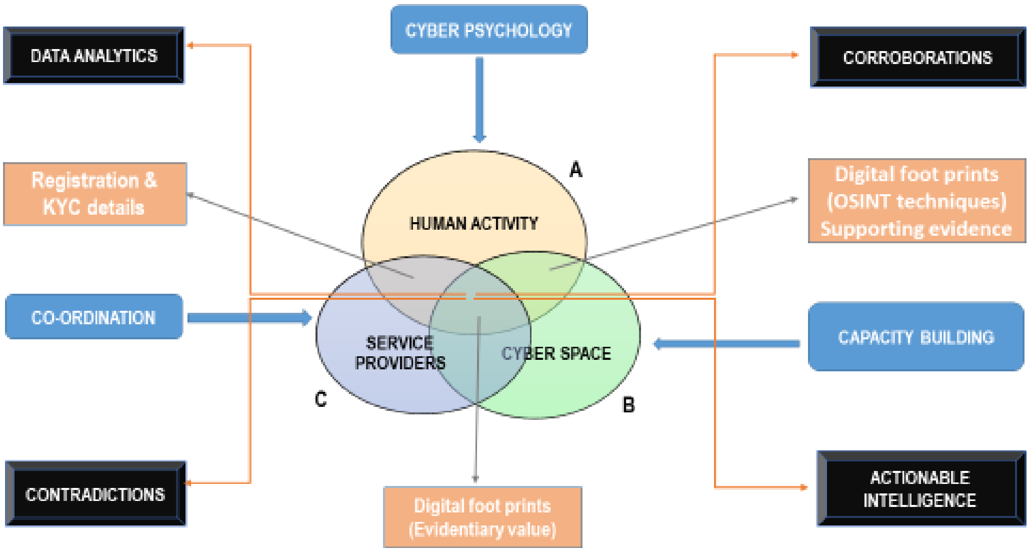
TYPES OF EVIDENCES


DIRECT
e.g. Witness testimony, CCTV footage, Audio Recordings
DIGITAL
CRIME SCENE EVIDENCE
DOCUMENTARY
e.g. PCs, Laptops, ITC devices, Mobile Phones, Internet services
e.g. Documents/ Records
INDIRECT
Circumstantial in nature

THE EVIDENCE LINKAGE PROCESS

Nagendar

INVESTIGATOR'S APPROACH



CYBER PSYCHOLOGY

DATA ANALYTICS

Registration & KYC details

CO-ORDINATION

CONTRADICTIONS

CORROBORATIONS

Digital foot prints (OSINT techniques) Supporting evidence

CAPACITY BUILDING

ACTIONABLE INTELLIGENCE

HUMAN ACTIVITY

A

SERVICE PROVIDERS

C

CYBER SPACE

B

Digital foot prints (Evidentiary value)

360° EVIDENCE = A+B+C

Nagendar

THE INVESTIGATOR'S PERSPECTIVE

- TUNNEL VISION:

RESTRICTIVE

Limits the scope of investigation

(UNIDIRECTIONAL –SINGLE MINDED)

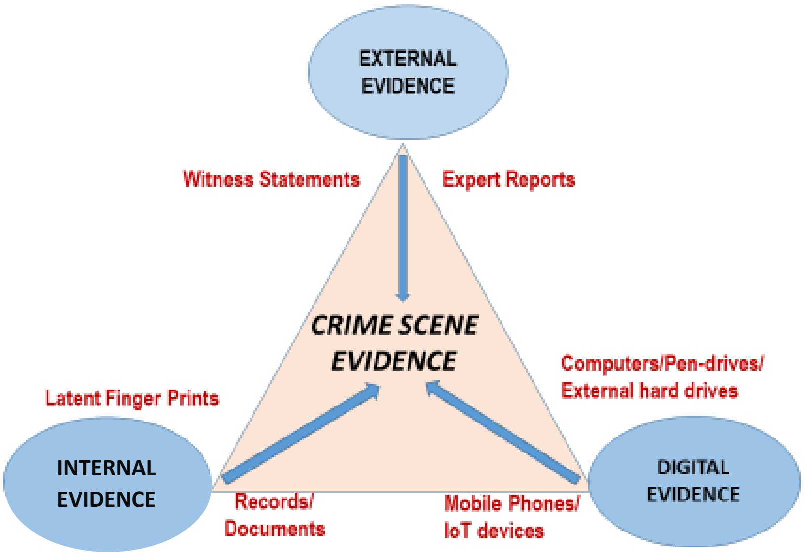
- FUNNEL VISION:

PROGRESSIVE

Broadens the scope of investigation

(MULTIDIRECTIONAL – EXAMINES VARIOUS ASPECTS) – 360° EVIDENCE

Nagendar



THE EVIDENCE LINKAGE TRIANGLE

Nagendar

ഇ❈ര

23. TEMPLATES

Certificate under Section 65-B of the Indian Evidence Act about DVR (Digital Voice Recorder)

It is certified that the conversation of the suspect official ………… (Name and designation) with the complainant …………. (Name and address) was recorded by the undersigned on XX-XX-XXXX (date) in the memory card through electronic devices ………… (Device description) in the presence of independent witness …………………… (Name and designation), as the undersigned was verifying officer of the complaint.

A Copy of the same conversation was also retained on the official laptop for investigation purposes, using forensic tools/procedures. The memory card ……………………… (Description) used for recording was then removed from DVR (digital voice recorder) and was sealed and marked as XX-XX.

It is further certified that at the time of recording of the above conversation, I had lawful custody over the DVR (Digital Voice Recorder) and laptop. The same was operating properly, and there was no operational problem. It is further certified that no changes have been made in the data while copying it on the official laptop.

It is further certified that the conditions in Section 65-B of the Indian Evidence Act, 1872 regarding the admissibility of electronic records in relation to the information in question are fully satisfied.

(Name & Designation of Official)

Certificate under Section 65-B of the Indian Evidence Act about CDR (Call Detail Records)

This is to certify that the information in the CDR of XXXXX (phone number) during XX-XX-XXX to XX-XX-XXXX (date), enclosed herewith, is a true extract of the relevant data created in the usual and ordinary course of business and stored on the designated hard disk of the computer systems of ……………(Company description) and/or its affiliate companies.

During the relevant period, the information of the kind contained in the electronic record, or of the kind from which the information so contained is derived, was regularly fed into the computer in the ordinary course of the said activities.

The computer output of the said information was produced by the computers during the period over which the computer/servers were used regularly to store and process information for the activities regularly carried on over that period by the officers of the Company, who had lawful control over the use of the computer.

During the relevant period, and to date, the computer/server is operating properly, and the printouts correctly contained the said information as recorded by the computer/server in the ordinary course of the said activities.

This certificate is signed on this XX-XX-XXXX (date).

(Name & Designation of Official)

Certificate under section 65-B of the Indian Evidence Act with regard to e-mail printout

This is to certify that I am ……………. (Name) and reside/work at …… I have an e-mail account vide ID ……….. Maintained with an e-mail service provider (ESP) ………………

The requisite details are as follows:

Electronic record: Description of the document to be proved (printout of e-mail and headers)

E-mail description:

ID …………………

ESP ………………..

Computer …………………

Make ………………..

Model ………………..

Serial Number ………………….

Software ………………….

Operating System …………………..

I certify with respect to the aforesaid electronic record printed from the above e-mail ID that,

The information contained in the above e-mail was fed, being sent/received in the ordinary course of activity/usage of the e-mail account, which was in my dominion/control.

During the period …………..to ………the abovementioned e-mail account was functioning properly, and there has been no such operational problem to affect the accuracy of the e-mail account or its contents.

During this period, the e-mail account was in my control and secured from unauthorized access, and the e-mail software has built-in security mechanisms.

The electronic record generated from the above e-mail has been derived from the information sent/received from it and is a true extract of the data from the aforesaid e-mail account.

The above said e-mail account is functioning securely and in my dominion/control, till today, i.e., ………………………, when the printout was taken from the aforesaid e-mail account. The printout of the e-mail and header have been taken directly from the e-mail account by accessing it from the computer system mentioned above.

I am personally involved in the transaction and /or generation of aforesaid electronic records.

The above-stated matter is true to the best of my knowledge and belief.

(Name & Contact Details)

CERTIFICATE U/S 2A OF BANKER'S BOOKS OF EVIDENCE ACT, 1891
(R/W 65-B OF INDIAN EVIDENCE ACT, 1872)

It is certified that the enclosed electronic record/computer output is the statement of SB A/c. No. __________________________of ______________________(name & address of the account holder) maintained with _______________(Bank & Branch) from____________to___________ in sheets serially numbered from 1 to ___ is the true extract in printed form of the relevant data created in the usual and ordinary course of business of the Bank and stored in the Bank's central server and the same has been retrieved from the computer systems/ central server of the bank located at_____________and that the data furnished is complete and true reproduction of the original data, to the best of my knowledge and belief.

It is further certified:

That the Access to the Computer System and the data stored thereon is controlled by defined authorized roles exercised through unique user-ID and the associated passwords. Only the concerned user knows the password, and the use of ID with a password establishes his identity and accountability. Changes to the data are controlled through application-level checks and controls;

That physical access to the computers/server is properly secured. Detection of any unauthorized changes in the data after day-end and before the day begins activity is carried through Check-sum procedures built into the application program. Unauthorized changes in the data during regular working hours are prevented/detected through verification of outputs with authorized inputs;

That the system verifies the backup during the process of transferring data to backup media and that physical and logical labels identify the data storage media; that backup devices and media are properly secured by the authorized personnel and are in the custody of a designated staff member; that physical and logical access controls are in place as safeguards against tampering of the systems.

It is further certified that to the best of my knowledge and belief, the Computer System that generated and stored this information operated properly at the time of such generation/storage of the data, and the printout represents the relevant data correctly.

Signature
(Name & Designation)
Emp. No.
Complete Address

Requisition To District Cyber Lab (CoE) For Visiting Crime Scene

PS __________.
Date __________

To
______________________________,

Sir,

Sub: - Request to depute Cyber Lab staff to the crime scene - Regarding.
Ref: - Cr. No.____ / 20 ____ U/S ______________ IPC of PS ________.

***

It is submitted that on ____________ the complaint Sri / Smt ___________, ________________ R/O ___________________________________ present a report / recorded statement wherein the complainant stated that (brief facts of the case)____.

As per the contents of the report a case in Cr. No.____ / 20 ____ U/S ______________ IPC was registered and investigation was taken up.

During the course of the investigation, the scene of offence was visited, and the following physical evidence is available at the scene:

1. Computer system (On/Off condition)
2. Laptop (On/Off condition)
3. Mobile phone (On/Off condition)
4. Printer
5. IPad
6. Pendrive
7. DVD/CDs
8. Other ICT devices of interest to the case

In this connection, it is requested to depute:

1. District Cyber forensic Lab experts from COE with suitable cyber forensics tools
2. The photographer/videographer to the crime scene.

Place:
Date:

Yours faithfully

(signature)

Name : ___________________
Rank : ___________________
PS : ___________________

DETAILS OF THE DIGITAL EVIDENCE

Crime Number…………………………………………   Date of
Seizure……………………………………………………
Name of the I.O……………………………………
Time…………………………………………………………………
P.F Number…………………………………………

TECHNICAL INFORMATION			
MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY					
REASON/ ACTON	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

24. SOPs – READY RECKONER

1) Abusive Mails

1. Collect the mail IDs of the sender/Victim
2. Address a mail to the concerned service provider to collect the IP logs of the sender/suspect mail ID
3. After collecting IP logs, analyze them using 'what is my IP address'
4. Send a mail to the concerned service provider to find out who used the particular IP address on that specific date and time
5. Correlate the emails as evidence
6. Identification and Arrest of accused and seize incriminating material
7. Interrogation of accused to find out previous offences, if any
8. Correlate the evidence collected
9. Forward the material to FSL and collect the Expert's report.
10. File the charge sheet as per approval

2) Abusive Calls /SMS

1. Collect the CDRs of both the numbers (victim/suspect) from the service provider
2. Collect IMEIs of the suspect and obtain the CDRs of numbers used
3. Analyze the CDR data, tower data, and IMEI data
4. Identify the location of the suspect based on CDR
5. Arrest the accused and seize the incriminating material
6. Interrogation of accused to know the details of previous offences
7. Connect the CDRs of the accused and victim as evidence
8. Correlate the evidence collected
9. File the charge sheet as per approval

3) Facebook

1. Collect the Facebook (FB) account ID/URL of the suspect/fake profile
2. Open the account, collect screenshots/URL of the account
3. Prepare a notice to FB and scan the notice copy
4. Send a mail to FB by attaching the scanned copy
5. After collecting FB replies, analyze IP logs
6. Trace the ISP through 'what is my IP address'
7. Send a notice to ISP for tracing the address, i.e., to whom the IP is allotted on a particular date and time
8. Arrest the accused and seize the incriminating material
9. Forward the material to FSL and collect the Expert's report
10. Correlate the evidence collected
11. File the charge sheet as per approval

4) Hacking of Mails

1. Collect the IP logs of the victim's mail ID by addressing a mail to the concerned service provider
2. After collecting IP logs, identify the service provider through "what is my IP address"
3. Send a mail to the concerned service provider to collect the details of the IP address used on that particular date and time
4. Identification and Arrest of accused and seizure of material
5. Correlate the evidence collected
6. Forward material to FSL and collect the Expert's report
7. File the charge sheet as per approval

5) For Debit/Credit cards fraud

1. Address a notice to the concerned bank of the complainant/victim for collecting bank statement of card transactions of a particular date and time
2. Whether the bank reverted the money to victim / complainant or not.
3. If the card transaction is done online. Request to furnish IP logs/ contact number of a fraudulent transaction (Bank alert number)
4. If the mobile number / IP address is furnished, then collect the CDRs / IP logs.
5. Conduct analysis of CDRs for tower details, frequently called/received numbers, and identify accused from service messages/requests, etc.
6. Collect/identify the information about the beneficiary merchant, account number, shopping mall, mobile number, etc.
7. If the beneficiary merchant account has an online banking facility, collect the IP details.
8. Conduct analysis for frequent callers, FB search, Google search, true caller, etc.
9. After collecting CDRs, the Physical address of the IP, correlate with the evidence collected.
10. Identify and arrest the accused; seize the incriminating material
11. Correlate the evidence collected
12. Forward the material to FSL and collect the Expert's report
13. File the charge sheet as per approval

6) Hacking of Bank Accounts

1. Address a notice to the concerned Bank to furnish the Victim's Bank account details
2. If the fraudulent transaction is an **online purchase**

a) Request the concerned to furnish fraudulent transaction IP logs with the date and time
b) Also, request to furnish the details of Gateway/merchant
c) Address a mail to gateway/merchant to furnish the IP/ mail ID/ contact details and mobile number.
d) After collecting IP logs, identify the service provider through 'what is my IP address'
e) Send a mail to the concerned service provider to collect the details of the IP address (to know who used the IP on that particular date and time)

3. If the mobile number is furnished, collect the CDRs and analyze tower details, frequent callers, etc.
4. Trace the accused from service messages/requests, etc.
5. Identify and Arrest the accused; seize the incriminating material
6. Correlate the evidence collected collected
7. Forward material to FSL and collect the Expert's report
8. File the charge sheet as per approval

7) Online Account Transfer

1. Address a notice to the concerned Bank to furnish the Victim's Bank account details
2. If the fraudulent transaction is **online transfer**
   a) Request the concerned to furnish fraudulent transaction IP logs with the date and time
   b) Also, request to furnish the beneficiary account details, viz., transaction details/account statement, CAF, introducer details, mobile number for alerts, etc.
   c) If the beneficiary account has an online banking facility, collect the IP details to trace the accused
   d) After collecting IP logs, identify the service provider through 'what is my IP address'
   e) Send a mail to the concerned service provider to collect the details of the IP address (to know who used the IP on that particular date and time)
3. If the mobile number is furnished, collect the CDRs and analyze tower details, frequent callers, etc.
4. Identify the accused from service messages/requests, etc.
5. Arrest the accused and seize incriminating material
6. Correlate the evidence collected
7. Forward material to FSL and collect the Expert's report
8. File the charge sheet as per approval

8) Lottery fraud / Nigerian fraud / Celebrity fraud/ Job Fraud

1. Identify the bank account and mobile numbers of the fraudster
2. Address a notice to the bank to furnish the details of beneficiary account viz., transaction details / Account statement, CAF, introducer details, mobile number for alerts
3. Collect the CDRs of fraudster numbers and analyze the same for tower details, frequent callers
4. Trace the accused from service messages/requests, etc.
5. After collecting the Bank details, verify the address of bank accounts and mobile number address
6. Cross-check the Bank Alert mobile number furnished by the bank with CDRs of the fraudster's mobile numbers and compare the towers and common numbers
7. Conduct analysis for frequent callers, FB search, Google search, true caller, etc.
8. Identify and Arrest the accused; seize incriminating material
9. Correlate the evidence collected
10. Forward the material to FSL and collect the Expert's report
11. File the charge sheet as per approval

25. CYBER CRIMES – CATEGORY: MAJOR, MINOR & SUB-HEADS

Sl No	**Category of Offence's**			**Sec of Law– Applicability**	**Description of the Offence**
	Major Head	**Minor Head**	**SubHead**		
1.	**Identify Theft** **Sec. 66 (C), 66 (D) IT Act, 420 IPC.**	Bank Related Frauds: Vishing (Call) Fraud Smishing (SMS) Fraud Phishing (e-mail) Fraud	Aadhaar Linkage PAN Card Linkage KYC updation Blocking of card Card limit - enhancement Reward Points Replacement of card - with photo/Chip Any Others	66 (C) IT Act and 420 IPC	A. Calling over the phone pretending as bank representatives, collecting bank A/c credentials like Card details, OTP, and misusing the same. B. Sending SMS/e-mail to the victim, collection of credentials of bank A/c, Card details, OTP, and misuse of the same.
		Skimming / Cloning of Cards etc.,	ATM Center Merchant Place	66 (C) IT Act and 420 IPC	Placing Skimmers at ATM Centers / collecting data at Merchant Places. Withdrawal of amounts with cloned cards from ATMs and from Merchant Places.

		Fake Customer Care Service Fraud	Google Just Dial Any Others	66 (C), 66 (D) IT Act, and 420 IPC	Posting fake customer care service Ads in Google, Just Dial, etc., in the name of original firms/companies and deceiving the victims in the name of fake Customer Care Services, etc., and taking huge amounts.
		Income Tax Fraud		66 (C) IT Act and 420 IPC	Personating as if from the Income Tax department and cheating the victims on the pretext of better return of tax paid amount etc.
		SIM SWAP Fraud		66 (C) & (D) IT Act and 420 IPC	Submitting forged documents and collecting/replacing SIM cards from Telecom Service Provider stores for committing bank fraud.
2.	**Online Frauds Sec. 66 (D) IT Act, 420 IPC.**	Job Fraud, Visa Fraud	Naukri Shine Monster Any Other	66 (D) IT Act and 420 IPC	Calls / Messages/e-mails are made/sent to the victims on the pretext of arranging a Job / Visa, etc., deceiving them by

					parting with money towards the Registration fee, advance fee, etc.
		Loan Fraud		66 (D) IT Act and 420 IPC	Personating as financial institutions and deceiving the victims on the pretext of arranging loans at a low rate of interest etc.
		Insurance Fraud		66 (D) IT Act and 420 IPC	Personating as insurance company representatives and deceiving the victims on the pretext of better insurance plans etc.,
		Lottery Fraud		66 (D) IT Act and 420 IPC	Either calling or sending SMS / e-mails to victims by mentioning that they have won a prize over lotteries organized by popular organizations and thus deceiving victims to part with money on the pretext of paying for an advance fee, getting no-objection certificates etc.

		Advertisement Portal Fraud	OLX Quikr CarDekho Facebook Instagram Any Other	66 (D) IT Act and 420 IPC	Posting fictitious/fake Ads in classifieds of Social Media Platforms and deceiving the victims.
		Gift Fraud (By using the name of e-Commerce platform)	Snapdeal Shopclues Amazon Flipkart Clubfactory Naaptol Home Shop 18 Any Other	66 (D) IT Act and 420 IPC	Securing customer data of e-commerce platforms and deceiving the customers on the pretext of winning Gift.
		Trading Fraud	Share Trade Forex Trade Commodity Trade Investment Advisors	66 (D) IT Act and 420 IPC	Cheating the victims on the pretext of fetching huge amounts on investing in Share / Forex / Commodity Trade / by paying amounts towards Share market Tips (IA's).
		Delivery of duplicate / Sub-standard products Fraud		66 (D) IT Act and 420 IPC	Cheating the victims by sending duplicate / Sub-standard articles to the victims instead of sending the original products shown online.
		Mobile Fancy Number Fraud		66 (D) IT Act and 420 IPC	Cheating the victim by offering fancy mobile numbers.

		Cell Tower Installation Fraud		66 (D) IT Act and 420 IPC	Personating cell companies and cheating the victims in the name of agreement with TSPs & victims and thereby parting with amounts in the name of an advance fee, security deposit, etc.
		Online relationship Fraud	Friendship through A). Matrimonial – Websites B). Social Media Platforms	66 (D) IT Act and 420 IPC	Posting attractive fake profiles over matrimonial websites / Social Media platforms once victims get attracted to such posts and after gaining faith collecting money on false pretexts.
		Dating / Female escort Fraud		66 (D) IT Act and 420 IPC	Cheating the victims in the name of dating / female escorts collecting amounts on the pretext of the Registration fee, membership fee, character verification fee, etc., for sexual favours.
		Business and Investment Fraud		66 (D) IT Act and 420 IPC	Cheating in the pretext of supply of raw materials, better returns in the short term, etc.

3	**Cyber Stalking** **Sec. 354 (D), 509, 506, 507 IPC and Sec.67 of IT Act.**	Stalking over 1. Social Media, 2. Classified Websites and 3. Pornographic Websites.	Facebook Instagram Dating Websites Porn Websites Any Other	354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creating a fake profile in the name and identities of the victim/sending add friend requests to victim friends, posting the mobile numbers of the victim on Classified / Pornographic Websites, etc.
		Stalking over 1. SMS 2. e-mails 3. WhatsApp (VOIP etc.,)		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Sending unsolicited e-mails and messages with abusive or objectionable contents.
		Stalking by fake Social Media Profiles.		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creation of fake profile over Social Media.
		Blackmailing, Intimidation, Sextortion.		354 (D), 506 / 507, 509 IPC, and 384 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creating a fake profile in the name and identities of the victim/sending add friend requests to the victim's friends coupled with a ransom demand.

		Cyber Flashing		354 (D) IPC and Sec.67 of IT Act.	Sending unsolicited obscene images/videos to the victims through a wireless convention channel.
4.	**Violation of Privacy** **Sec.66(E) IT Act, 354 (C) IPC.**	Taking images through phones.		66-E IT Act, 354 -C IPC (Depending on the case)	Taking images of private parts and activities of people over mobiles phones etc.,
		Taking photos with hidden cameras.		66-E IT Act, 354 -C IPC (Depending on the case)	Keeping hidden cameras and capturing images of private parts at bathrooms, trial rooms, etc.,
5	**Cyber Pornography** **Sec.67, 67 (A) IT Act.**	Circulation of obscene images / text.		67 IT Act	Circulation of obscene images or sending obscene text messages over SMS or WhatsApp.
		Circulation of Obscene videos.		67 and 67-A IT Act	Circulation of obscene videos over Social Media, e-mails or WhatsApp.
6	**Child Pornography** **Sec.67, 67 (B) IT Act, POCSO Act.**	Circulation of Obscene child porno		67, 67 (B) IT Act and POCSO Act	Circulation of obscene videos related to children over social media, e-mails, or WhatsApp or downloading child sexual porno, enticing children for online relationships, etc.

7	**Source Code Tampering** **Sec.65 IT Act**	Stealing, deletion, and destruction of source code		65 IT Act	Stealing of computer programme/application/ code and using self or for others.
8.	**General Computer Offences** **Sec. 66 r/w.43 IT Act, 384 IPC.**	Hacking		66 r/w. 43 IT Act	E-mail ID, FB Profile Hacking and misuse, Server computer hacking by changing password, etc.
		Business e-mail ID compromise Fraud		66 r/w. 43 IT Act	Compromising business e-mail IDs, interception of data, sending deceptive e-mails for committing Fraud, etc.
		RansomWare		66 r/w. 43 IT Act and 384 IPC	Taking control of a computer system or server by sending malware and demanding money to release.
9.	**Online IPR Offences Sec.66 (B), 65 IT Act.**	CopyRights violation over Internet		66-B, 65 IT Act and Copy Right Act	Movie uploads, copyright contents uploads.
10.	**Communal content over Social Media** **Sec. 153 (A), 505 IPC.**	153-A (Depending on the nature of offence), 505 IPC relevant Sub-Sections		Morphing images of gods and goddesses and items of religious importance, circulation over social media and/or making communal sensitive statements over social media.	Communal content over social media

26. DIGITAL INTELLIGENCE – BASIC OSINT TOOLS

Digital Intelligence (DI) has something to do with the skills needed to use technology more effectively. It’s not just being aware of vulnerabilities with overuse screens or knowing when to disconnect from your device; digital intelligence must include debugging a computer or using all the smartphone features, checking from whom the mail came from, checking the correct mail headers, etc.

DI will become vital for developing digital skills and profiles in this 21st Century digital age. There are eight basic DI principles, and they are

1) Identity – Managing a healthy online identity
2) Use – Self-monitoring screen-time usage
3) Security – Identifying situations of harassment and managing them
4) Protection – Detect threats and establish best practices, i.e., malware, etc.
5) Privacy – Sharing of personal information discreetly
6) Critical Thinking – Distinguish between true and false
7) Finger Prints – Managing online presence responsibly, knowing long-term consequences,
8) Empathy – Feelings of both yourself and others.

Below are a few digital intelligence tools for investigation purposes

1) **Exodus** analyses Android applications. It looks for embedded trackers and lists them. It does not decompile applications, and its analysis technique is entirely legal. https://reports.exodus-privacy.eu.org/en/
2) **Lightbeam** for Chrome uses interactive visualizations to show users the relationship with third parties, i.e., how corporates share data. https://myshadow.org/resources/lightbeam?locale=en
3) **Have I Been Pwned** searches multiple data breaches to determine whether your email address or phone number has been compromised or leaked? https://haveibeenpwned.com
4) **The OSINT framework** is designed to gather information from freely available tools or resources. The intention is to help people find free OSINT resources. https://osintframework.com
5) Allowing subscribers to confirm their registered numbers and remove numbers that were registered without their knowledge.https://tafcop.dgtelecom.gov.in
6) Open Source data collections by security professionals and forensic investigators — https://www.maltego.com/

7) We can view the following information: location history, device information, voice and audio activity, YouTube Search History, and YouTube Watch History.https://myactivity.google.com

8) **Namechk** checks domain name and username on dozens of social channels and online platforms.https://namechk.com/

9) **TinEye** is an image search and recognition company. In simple terms, it's a way of fact-checking an image published online (Reverse Image Check). https://www.tineye.com

10) **View Exif Data** is a tool for extracting the Exif metadata that is embedded in photos taken with digital cameras and stored as images; we can get (Date / Camera / Location etc., where it was taken). https://exifdata.com/

11) To check complete URL details of short links. https://www.unshorten.it

12) **Isitphishing** service assists in protecting identity, data, and computers from threats and viruses; we can check if a website is engaging in phishing activity. https://isitphishing.org/

13) This tool will make email headers human readable. We can check the complete email header. https://mxtoolbox.com/EmailHeaders.aspx

14) Research domain ownership with **Whois Lookup**, i.e., get ownership info, IP address history, rank, traffic, SEO & more. http://whois.domaintools.com/

15) **Archive-It** enables capturing, managing, and searching digital content collections without any technical expertise or hosting facilities. Check the old version of the target website. https://archive.org/web

16) Allowing subscribers to identify the sender of bulk SMS.https://smsheader.trai.gov.in/

17) **Platform** for determining whether the video was genuine or a deep fake. https://platform.sensity.ai/deepfake-detection

Other Websites for Investigation			
1.	www.whatismyipaddress.com	11.	www.images.google.com
2.	www.numberingplans.com	12.	www.photobucket.com
3.	www.whois.com	13.	www.tracersinfo.com
4.	www.tineye.com	14.	Maps.google.com
5.	www.virustotal.com	15.	www.internet101.org
6.	www.pipl.com	16.	www.knowem.com
7.	www.spokeo.com	17.	www.whostalkin.com
8.	www.domaintools.com	18.	www.socialmention.com
9.	www.traceroute.org	19.	www.internetfrog.com
10.	www.mapquest.com	20.	www.mapquest.com

27. FAKE NEWS & FACT CHECKING

Understand the terms of fake news:

- **Misinformation:** Information that is false, but the person who is disseminating it believes that it is true.
- **Disinformation:** Information that is false, and the person who is disseminating it knows it is false. It is deliberate, intentional.

Types of fake news:

- **False Connection:** When headlines, visuals, or captions don't support the content.
- **False Context:** When genuine content is shared with false contextual information.
- **Manipulated Content:** When genuine information or imagery is manipulated to deceive
- **Satire or Parody:** No Intention to cause harm but has potential to fool.
- **Imposter Content:** When genuine sources are impersonated.
- **Fabricated Content:** Content that is 100% False designed to deceive and do harm.
- **Propaganda:** When content is used to manage attitudes, values and knowledge.
- **Sponsored Content:** Advertising or PR disguised as editorial content.

How to filter the fake news on social media & internet:

- **Source:** Consider the source from a reputed news channel or newspaper only, do not rely on forwarded messages on social media.
- **Website URL:** Check if it is legitimate, i.e. (gov. in for government,.edu for education, etc.)
- **Author:** Check who's the Author and his credibility in the past. Fake ones do not have their names and signature.
- **Headline:** Read beyond the headline, meaning read the entire article to understand the viewpoint and tone of the message or article.
- **Disregard your bias:** Many people watch news or stories that confirm their own beliefs or biases, and fake news can prey on these biases.
- **Get a Second Opinion:** If a story makes you angry, dig deeper, consult a known contact or consult fact-checking agencies like www.factly.com

Basic Fact Checking:

- Do a reverse image search Offered by: www.google.com & http://www.tineye.com/
- Photo / Image / Video verification – using INVID tools (Browser Extension Tools – Please download the Browser Extensions) https://www.invid-project.eu/tools-and-services/invid-verification-plugin/
- Fact Check before forwarding, i.e., www.factly.com
- Don't forward any content that You Don't Own.
- Don't click or any unknown emails / attachments / links / maps. Scammers are using Phishing Tactics in the name of Charity, Help Desks, Maps, etc., to steal identity or money.

28. REFER - INVESTIGATOR'S DIRECTORY

(Cyber Warriors Series-2.0)

Office of the
Director General of Police,
Telangana State, Hyderabad.

Rc.No.128/Plg.1/2019
C. No. 107/PSQMU/TS/2019 Dt. 10.08.2019

CIRCULAR MEMORANDUM

Sub: TS Police – Centres of Excellence (CoEs) at Unit Level- Uniform Delivery of Services in all Units - Setting-up of Centres of Excellence (CoEs) in all Districts / Units to provide support services in real-time to all Functional Verticals – Operational Standards defined and Communicated– Reg.

* * *

Technology Innovation in Police work has been the focal point of Telangana State Police since the inception of State of Telangana, whether it is CCTV Surveillance System, Traffic Management System, or Mobile Apps etc., to Support Strategic Police Initiatives. Implementation of New Technological Innovations has been the cornerstone of evolution and reform in Telangana Police.

The adoption of sophisticated technologies by Telangana Police has resulted in enhancing operational effectiveness in the maintenance of Public Order and Peace, Crime Prevention & Investigation, Intelligence Gathering, Faster Response to Emergency Situations, Improving Traffic Compliance, Enhancing the Strong Relationships with Local Communities, etc.

The primary focus of these Technological Innovations has been:

- Developing an overall strategy for strengthening crime control efforts by improving the ability of police to identify and monitor offenders
- Expediting the detection and response to crimes, enhancing evidence collection abilities, and improving police strategies
- Enhancing communication between police and citizens
- Strengthening the ability of law enforcement to deal with technologically sophisticated forms of crime

In order to bring about these efforts into a Systemic Frame Work, it is proposed to establish Centres of Excellence (CoEs) in all Districts/ Police Commissionerates to render support services on a 24/7 basis to all the frontline Police Officers, Investigating Officers and Supervisory Officers for strengthening Investigation and Crime Prevention efforts.

The proposed Centres of Excellence (CoEs) include:

i) Integrated Command & Control Centres (ICCC CoE)
ii) Cyber Forensic Lab (CFL CoE)
iii) Mobile Clues Team (MCT CoE)

iv) Video Enhancement Lab (VEL CoE)
v) Data Analytics Unit (DAU CoE)
vi) Social Media Monitoring Unit (SMU CoE)
vii) Hotspots and Root Cause Analysis Unit (HRAU CoE)

ROLE OF CENTER OF EXCELLENCE (CoE)

Each Center of Excellence (CoE) aims at enhancing quality service delivery and promote uniformity and standardization of operations, coordination and conformity to policing values amongst the delivery units. Each CoE is to empower the concerned functional Verticals to get the most out of the technology, not only within teams but across the entire department. A CoE associates the long-term strategy with the day-to-day operations, documenting lessons learnt, evolve best practices, and makes it easier for different groups to reuse and adapt proven solutions.

It will facilitate strengthening all Functional Verticals at Police Station Level to achieve the following core objectives within the department:

- Maximum utilization of common infrastructure; video-based systems and Information Technology (IT) based applications and databases.
- Process optimization & standardization; establishing & promoting best practices.
- Build multi-functional knowledgeable articulated capabilities, and expertise in domain & technology.
- Optimize & enhance resources utilization and leveraging reusable assets
- Providing situational awareness and actionable intelligence to the field & supervisory officers
- Reducing delivery times and increasing efficiencies
- Measuring Performance and establishing a feedback mechanism

1. INTEGRATED COMMAND & CONTROL CENTER (ICCC CoE)

The Government of Telangana has taken up an initiative to set up an Integrated Command & Control Centre at State headquarters with a state-wide CCTV Surveillance System. Over 5,13,593 CCTV Cameras have come up in Telangana so far with the help of community support as envisaged under the provision of the TS Public Safety (Measures) Enforcement Act. The efforts to add CCTV Cameras in Local Communities shall be an ongoing process.

When all the Unit Command & Control Centres (UCCC) for Law & Order and Traffic are established in all District / Commissionerates of Police, they will be connected to the Central Command & Control Centre at the State headquarters, thus will start working in tandem as Integrated Command & Control Center (ICCC). It provides access to a wide variety of structured and unstructured data from various sources, such as combined information on detection of crime and criminal data, incidents from Dial-100, Hawkeye App, Road accidents, State-wide Surveillance Cameras, Patrol Vehicles tracking data, Traffic enforcement data, and data from Social media platform to improve response times through aggregation, correlation analysis, and dissemination of actionable information to the field officers. It is a collaborative effort of multiple agencies to provide resources, expertise, and information with the goal of maximising their ability to detect, prevent, investigate and respond to any emergency/crime incidents and threat activities.

The officers identified for deployment at the ICCC must be trained in necessary skills as it is the nerve centre for both Law & Order (L&O) and Traffic operations. Seamless coordination between the L&O and Traffic will result in better execution of police functions.

To reap good results, the ICCC must be structured based on the standards necessary to run the centre 24/7.

The ICCC is used for:

- Linking vital systems and communications – not just to gather information, but also to allow seamless communication of critical instructions, notifications and alerts.
- The surveillance system, resource management, and public information systems will be correlated for effective monitoring and efficient policing.
- Increasing the geographical and situational awareness by providing insights using video feeds and IT data from field edge devices and sensors for field and supervisory officers across various functions within the department.
- Standardizing response protocol through the institutionalization of standard processes for recurring events, issues and exigency scenarios.
- Providing automatic and adaptive workflows for effective situation management; enforcing procedures through Standard Operating Procedures (SOPs) and ensuring compliance.
- Enhancing collaboration within Wings and across Departments (multi-agency).
- Institutionalizing evidence-based and information driven decision making from single source of information for regular operations across the organization.
- Engaging with on-field support staff to address various issues and citizen grievances.
- Ability to receive, intelligently correlate and share the information with internal and external stakeholders to enhance operational efficiency.
- Enhancing safety, security and providing better public services for better and healthy relationships with the citizens and communities.

A. Law & Order Command and Control Centre:

The Law & Order wing of Police deals with a wide range of incidents and operations that require an authority to command its' personnel and use of its resources in an effective and efficient manner. The ICCC operated by L&O at all the Districts / Commissionerates of Police will be used to resolve incidents and control the operations ranging from the policing of a local community event to a major criminal investigation. Its main purpose is to provide accurate, complete and timely information to various ranks of officers.

It will empower the field operations teams by providing Geographical awareness, Situational awareness, centralised and controlled overall operations of the organisation and help in taking the appropriate decisions. Further, these centres will host shared services, Centres of Excellence, etc. of individual units.

The Operational Standards of L&O Command and Control Centre are:

- Gathering of information from various sources such as police stations, field, open source etc.
- Verification, correlation, and confirmation of collected information
- Evaluation and analysis of collected data in a meaningful way to suit the needs of the filed/Investigating Officer (IO)
- Categorization, documentation and storage of collected information in chronological order for easy reference
- Target tracking based on inputs and coordination with field staff/officer
- Prioritize information and communicate to all concerned based on the need-to-know basis (Senior Officers, Field officers, other officers/vertical staff etc.)
- Provide assistance in situational readiness and deployment of workforce during major events/operations
- Act as a quick and immediate response centre
- Sending early warning alerts to the concerned staff/officers through SMS and voice messages
- Maintaining a proper incident response mechanism for various types of incidents
- Every alert that is received has to be attended to within a time frame
- Real-time monitoring of critical/important public places regularly through CCTVs and by other means
- Coordinating with the local civic authorities such as local municipality/gram panchayat, hospital, fire station etc., in times of need for quick resolution of the problem

i) Resources:

Details of the proposed strength of L&O manpower for managing and working at the Command and Control Centre are furnished below:

DSP / Inspector	SI / ASI	HC / PC	Support Staff	TOTAL
1	3	6	2	12

B. Traffic Command and Control Centre:

The objective of ICCC operated by the Traffic wing is to act as a focal point for communicating traffic flow information to the field officers, patrol mobiles and monitoring traffic compliance by the public.

The Traffic Command & Control Centre is responsible for the receiving and dissemination of information on all matters relating to smooth and smart traffic management, traffic education & awareness, traffic rules enforcement, road accidents etc. It is integrated with the e-Challan System, where the images of violations are processed and the challans automatically mailed to the violators.

The Operational Standards of Traffic Command and Control Centre are:

- Ensuring traffic safety, smooth traffic flow, reducing travel time and enhancement of road-user experience
- Traffic enforcement by detection of traffic violations i.e. speed violations, red-light violations, parking violations etc.
- Surveillance, control & regularise traffic through display systems viz., Variable Message Sign (VMS) and Public Address Systems (PAS)
- Displaying real-time information to road users like speed limit, traffic flow, congestion, diversion points, road closures, alternative routes, weather conditions etc.
- Continuous observation of feeds from the CCTVs installed at various junctions, important/sensitive areas and highway corridors
- Every alert that is received has to be attended to within a time frame
- Providing real-time predictive traffic analysis to the filed officers/patrol mobiles based on the inputs
- Detecting vehicle locations, vehicle speeds, sensing road surface conditions sharing the information with the traffic field officers/patrol mobiles
- Identifying blind spots on the roads and sensitizing the road users/stakeholders
- Ensuring minimum response time of patrol mobiles in case of emergency situations
- Tracking of special vehicles like identification of hot-listed vehicles such as vehicles involved in bodily offences, traffic offences, theft, and other offences
- Management of mega-events like religious processions, student/political rallies, demonstrations, etc.

- Clearing way for emergency vehicles such as Fire Engines, Ambulance etc.
- Area-wise real-time collection of traffic data, consolidation and analysis for various requirements and decision making. The collected data is to be stored in chronological order for future references
- Conducting pattern analysis on-road incidents and sharing the intelligence to the concerned officers
- Act as coordinating centre during emergency situations and maintain liaison with civic authorities/stakeholders for effective addressing of the complaints, incident clearance and resolving emergency/critical issues
- Maintaining incident response mechanism for different types of traffic/road incidents
- Preparing special incident reports/annual reports for awareness and statistical purposes

ii) Resources:

Details of the proposed strength of Traffic manpower for managing and working at the Command and Control Centre are furnished below:

DSP / Inspector	SI / ASI	HC / PC	Support Staff	TOTAL
1	3	6	2	12

2. CYBER FORENSIC LAB (CFL CoE)

Today, Cyber forensic tools are one of the main analytical technologies used by the Police for investigative purposes. The Police are the first responder to the crime scene and their prime duty is to protect, collect and preserve the evidence for further analysis and investigation. Cybercrime cases are posing several challenges in prevention, detection, investigation and successful prosecution.

The main purpose of setting-up of the Cyber Forensic Lab is to examine and analyse computer / digital evidence for identification, collection, and preservation of evidence.

Cybercrime manifests itself in different forms such as online financial frauds, data theft, online stalking/harassment, defacement of government websites, industrial espionage, hacking, cyber terrorism etc., which requires specialised investigative skill set and cyber tools for analysis. Day-by-day, cybercrimes, cybersecurity risks and other challenges are growing manifold, hence there is an imperative need for police to keep pace with the latest cyber technologies and forensic tools.

The Operational Standards of the Cyber Forensics Lab are:

- Assisting the Investigating Officer (IO)/field staff in the identification, collection, and preservation of digital evidence in a way that preserves the integrity of the evidence

- Analysing the collected evidence and give inputs to the IOs and concerned staff
- Helping the IOs in forwarding the material objects to Forensic Science Lab for analysis
- Collecting intelligence regarding cybercrimes and sharing the same to all SHOs
- Conducting cyber-related awareness campaigns for officers and men on cybersecurity and information security
- Following the best practices to achieve good and productive results
- Documenting the cases received in the Lab along with the analysis report in a chronological order
- Guiding and facilitating Investigation Officers (IOs) in cybercrime investigation and in deposing evidence during the trial of the case
- Participating in cybercrime interrogations, prepare and preserve interrogation reports for future reference
- Documenting both hardware & software of the Lab and maintenance of the cyber forensic tools

i) Resources:

The personnel who have been trained and acquired sufficient skills in the usage of cyber forensic tools should only be posted to work in Cyber Forensics Lab. Continuous training on usage of the latest versions of tools and the refreshers courses will be organised for them to maintain the standards necessary to run the Lab.

The Police should always be prepared and ready to prevent cybercrime, cybersecurity risks etc. Hence, the select staff has to be imparted necessary training in using cyber tools and made self-reliant to support police officers while facing challenges during the investigating process.

Details of proposed strength for managing and working in the Cyber Forensics Lab are furnished below:

Inspector / SI	HC / PC	Support staff	Total
1	4	1	6

3. MOBILE CLUES TEAM (MCT CoE)

Crimes are committed by means of tools or weapons or things. These can be used as a vehicle to reach the crime scene. However, cautious a criminal may be, in the process of committing a crime, he leaves some physical evidence/marks at the crime scene such as fingerprints, footprints, body fluids, tool marks etc., which will stand against him. The evidence left by the criminal at the scene of the crime may be visible or partially visible which makes it difficult for the Investigating Officer (IO) for collecting evidence without appropriate tools.

The role of the Mobile Clues Team is to assist the Investigation Officers in methods of securing the crime scene prior to arrival; to document the crime scene with photography, video; to ensure the proper identification, handling, collection and packaging of physical evidence found at a scene; and to perform speciality examinations that would aid in reconstructing the events of the crime and thereby record and retrieve the vital physical evidence (material objects) that establishes the connection between the perpetrator and the scene of offence or the victim in all offences occurring in Telangana.

The Mobile Clues Team forensic experts fill the gap between the Investigator and Scientists of FSL by adopting proper collection methods and reconstruction of the scene thereby provide investigative leads for the detection of crimes namely, property & bodily offences, fire accidents and the scene of explosion etc. Its' presence in crime scene processing is vital. The functioning of the Clues team is aimed at improving the detection levels of crimes and improvement of conviction rates in the court of law and thereby improves the standards of safety and security of people living in Telangana.

The Operational Standards of the Mobile Clues Team are:

- Reaching the crime scene in the shortest possible time. So, the data could be collected first-hand before it is tampered /damaged
- Helping the Investigating Officer (IO) in cordoning and protection of the crime scene
- Documenting the entire crime scene by Photographing and Video recording
- Drawing sketch of the crime scene in a scientific manner detailing all the factors relevant for crime investigation
- Conducting a systematic search of the crime scene for physical evidence
- Proper Identification, handling and collection of physical evidence
- Proper labelling, marking of evidence and preparing the Letter of Advice
- Proper preservation and packing of the physical evidence for forwarding to Forensic Science Laboratories
- On the spot preliminary analysis of the collected physical evidence and providing leads to Investigating Officer (IO)
- Coordinating with the Medical Officers and other Scientific Experts visiting the crime scene
- Helping the Investigation Officer (IO) in the reconstruction of the crime scene
- Establishing the link between the crime scene and the criminal/suspect
- Conducting causative factors analysis in case of road accidents
- Scientific evidence collection using tools and guiding the Investigating Officer (IO) in the investigation of crime
- Documenting both hardware & software of the Lab and maintenance of the tools

i) Resources:

The select staff having necessary academic qualifications in science and having knowledge and trained in scientific aids are to be posted in Clues Lab. Further, sufficient number of Clues Teams need to be formed at District/Commissionerate level to support the functioning of the Lab.

Details of proposed strength for managing and working in the Clues Lab are furnished below:

Scientific Officer	Photographer-cum-Videographer	HC/PC	Support staff	Total
1	1	3	1	6

4. VIDEO ENHANCEMENT LAB (VEL CoE)

Unlike other forms of forensic evidence, audio and video recordings can provide a real-time, eyewitness account of a crime. Over a period of time, the assistance of video evidence in crime investigation has increased manifold. Nowadays, Audio and video evidence can be found at more locations and from more diverse sources than before. For instance, CCTV systems and video recorders can be found in business centres, at traffic junctions, parking lots, banks, etc.

The main purpose of the Video Enhancement Lab is to assist Investigating Officers (IOs), clarify or enhance and analyse video recordings using various scientific tools. For most cases, high-quality video recordings are often not available. Enhancing such video footage will provide a clear picture of what happened at the crime scene, which will help the Investigating Officer (IO) to properly detect and investigate the case. Further, video evidence also plays a vital role in finding, identifying the criminals & crime vehicles and in bringing conviction of cases, while at the same time, it protects the innocent persons from allegations.

The Operational Standards of the Video Enhancement Lab are:

- Receiving the video footages from the police officers and assigning a lab serial number to it for easy reference
- Before enhancement of video footage, first understand the modus operandi of the crime as it gives a better idea and approach for conducting analysis
- For better workstation functioning, every time take 5 to 10 minutes duration of video file for examination and enhancement purpose
- Conducting frame by frame matching of the video footage for better identification of suspect image/number
- Mixing of different frames of video footage for enhanced results.
- Matching the enhanced video footage results with available databases such as RTA database, e-challan system, social media applications like Facebook etc.

- Work patiently and diligently while analysing the video footages for better results
- Documenting the case-wise details with details like unit name, crime no., section of law, offence timings and analysis results (detected/undetected) in chronological order for easy reference
- Conducting training to the police officers and field staff on the identification of video-related evidence in the crime scene, retrieving the video footage from DVR/NVR systems, preservation of evidence, proper chain of custody, documentation of crime scene, etc.
- Helping the IO in the reconstruction of the crime scene
- Establishing the link between the crime scene and criminals/suspects
- Preparing periodical reports and sharing the relevant information to all the concerned officers

i) Resources:

The select staff having knowledge and trained in Adobe Photoshop, Video editing, Multimedia have to be posted in Video Enhancement Lab.
Details of proposed strength for managing and working in the Video Enhancement Lab are furnished below:

SI	HC / PC	support staff	Total
1	2	1	4

5. DATA ANALYTICS UNIT (DAU CoE)

Data analytics is an important tool for law enforcement to reduce crime epidemics. The main objective of this Unit is to act as a backbone and data collecting & building centre to the Police Department. Proper visualization, utilization and communication of data enhance the problem-solving capacity of the police. Insights gained from the right kind of data will help law enforcement approach problems in the most effective and efficient way. It also helps in maintaining the legitimacy with the community and thereby improvement in day-to-day police functions.

Data Analytics has the potential to predict patterns & trends and recognize suspicious behaviour & activities. Integration of data from various sources such as CCTV, traffic control, biometrics, command and control centre, social media applications, and open source will not only enrich the database but also helps in decision making, crime analysis and predictive policing.

The Operational Standards of the Data Analytics Unit are:

- Collecting data from various sources such as Police Stations of the district, DCRB/CCRB, SCRB, CCS, Special Branch, Fingerprint Unit, neighbouring states, CCTVs, Command Control, Service Providers, open-source data etc.

- Maintaining, updating and integration of data pertaining to various modules like crime, traffic, law & order, social media etc.
- Modus operandi-wise, maintaining the data of arrested persons/jail released persons and periodically inform the same to all police stations, CCS, DCRB/CCRB
- Categorization and storage of collected information in chronological order for easy reference
- After analysis, forwarding the relevant data/actionable intelligence to other Centres of Excellence
- Identifying the problematic areas of intensity and disseminating the same to the concerned officers
- Sharing of information on current trends related to law & order, crime and other factors of interest to the concerned officers/vertical staff
- Preparing quarterly, half-yearly and annual reports on various issues relevant to policing
- Helping the Investigating Officers and field staff in the investigation of cases and enquiries

i) Resources:

The select staff having knowledge in MS Excel, SQL, and Hadoop are to be posted in the Data Analytics Unit (DAU).

Details of proposed strength for managing and working in the Data Analytics Unit are furnished below:

Inspector / SI	HC / PC	support staff	Total
1	3	1	5

6. SOCIAL MEDIA UNIT (SMU CoE)

Today, Information Communication Technologies (ICTs) and mobile-based communications are increasingly become pervasive and integral to day-to-day functions of our lives. One of such technologies is Social Media. It is transforming the way in which people connect with each other and it has redefined the way in which information is shared and distributed. Day-by-day, it is gaining popularity and presenting an opportunity of connecting to each and every individual. Thus, it has become an effective communication channel for the Police to reach the community and serve them in a better way.

Community involvement and support is an essential pre-requisite for the success of policing. The interaction between the Police and the Community in real-time on a regular basis will help the Police improve its service delivery standards on a continual basis. In the line of Police duty, Social Media can be used as a community policing tool to reap the benefits of positive representation in the community, improved community communication and effective community policing.

Social media tools helps in facilitating Police to keep an eye on critical issues which are being discussed regularly among citizens on the Internet and to bridge the gap between the expectations of the public and delivery of police services. The objective is to make the citizen feel the presence of policing system by responding promptly to each and every post/complaint received on Social Media. Also, act in response to any instance of the day by posting, sharing, and updating information to ensure citizen safety.

Hence, setting up of a Social Media Unit (SMU) is essential to transform Telangana State Police into a Citizen Friendly and Responsive Police.

The Operational Standards of the Social Media Unit are:

- Monitoring, Collection and Receiving information posted on Social Media applications like Facebook, Twitter, WhatsApp etc., about police actions felt needs and public grievances related to Law & Order, Traffic etc.
- Highlighting all service delivery activities undertaken by police, police achievements, good work done by citizens etc., on a daily basis through social Media.
- Forwarding complaints/public grievances and relevant messages to the concerned Police Station for taking necessary action; also revert to the Citizens with status on complaint and remarks.
- Maintaining the database of the received complaints along with its disposal in a chronological order for easy reference
- Creating awareness among the citizens on precautions to be taken in various types of crimes, police activities, and safety & security
- Posting advisories on Law & Order issues, Traffic, Festivals etc., and Releasing press notes
- Generating monthly reports on Law & Order complaints, other issues, and their disposal
- Replying to citizen’s queries within the set time and giving them proper guidance
- Sharing adverse reports against policing, suspicious activities/Viral videos on Social Media with the concerned Police Officers/Verticals for necessary action

- Encouraging the Local Communities to enrol themselves as active Partners in policing activities through community policing initiatives in their respective Police Statin Areas
- Guiding the local Police Stations to transform themselves into tech-savvy Police Organizations and be a part of modern-day community interfaces.
- Assessing the citizen satisfaction levels with regard to various services provided by the local Police Stations from time to time.
- Coordinating with PRO, Police Stations and other Offices for collection of time to time updates
- Performing Admin functions with rights to access and monitor all the PS Facebook Pages & Twitter handles; maintenance of Facebook account and Twitter account

i) Resources:

The select staff having technical knowledge in handling of Social Media applications like Facebook, Twitter, WhatsApp, Hawkeye and other similar apps are to be posted in the Social media Unit (SMU). Further, the team members are to be trained in requisite soft skills and other skills relating to language, Reporting, Coordination, Answering, etc.

Details of proposed strength for managing and working in the Social Media Unit are furnished below:

Inspector/ SI	HC/PC	Support staff	Total
1	3	1	5

7. HOTSPOT & ROOT CAUSE ANALYSIS UNIT (HRAU CoE)

Timely and accurate analysis of crime data is critical to understand the driving factors of crime phenomena. Analysis of factors such as times and locations of criminal activity with that of the location of parolees, known criminals, gang members and socio-demographic data of criminals such as age, sex, address is essential in producing actionable intelligence leads, predictive analysis and for decision making.

The main purpose of the Hotspots & Root Cause Analysis Unit is to identify and address the root causes of crime and how to prevent criminal activity before it occurs once again.

The route cause analysis of crime on data collected from various sources helps in understanding identifying, hotspots, modus operandi, crime trends, finding missing links and establish links between criminals and the crime scene. This will further help in dealing with the crime more effectively, preparing for new challenges and in developing crime and risk reduction strategies.

Crime Analytics with Police Department is currently limited to crime counting and there is a greater need to police to move beyond counting to more sophisticated Crime Analysis. Hotspots and Root Cause Analysis Units are equipped with better tools to understand and analyse the incidents. These tools not only present the data in visual formats to help police detect the patterns but can help in crime forecasting. Hotspots and Root Cause Analysis Unit can identify the repeat victims or high-risk jurisdictions along with root causes and generate reports or crime bulletin for the police officers. This unit enables police to identify trouble spots and target appropriate resources to fight crime strategically. The result is computer-generated reports illustrating where and when a crime is occurring. With this 'pin-mapping' approach, the police can quickly identify crime-ridden areas and fashion a comprehensive response in partnership with local communities and other Government Departments.

The Operational Standards of the Hotspots and Root Cause Analysis Unit are:

- Generation of Crime statistics and Crime History marking the incidents on maps with the integration of crime records police station wise, circle wise, sub-division wise for understanding the crime patterns and design crime prevention interventions.
- Hotspot Identification based on Crime Statistics/History followed by Root Cause Analysis with the help of front line police officers of the concerned jurisdictions.
- Generation of Reports on measures to eliminate root causes in consultations with frontline police officers and their effectiveness over a period of time reducing crime.
- Collating and analysing the data of Dial 100 System to measure the extent of effectiveness of response by Police in urban, semi-urban & rural areas and circulation of reports to the police officers for ensuring compliance of target response. In case of any deviations, a gap analysis report to be sent to the concerned supervisory officer for taking necessary measures
- Analysis reports generation in respect of petty cases booked police station wise to understand the increase/decrease of a pattern of petty cases and outcome of booking petty cases
- Regular update of information to be geo-tagged and preparation of reports on GPS enabled MO offenders & History sheeters, Jail releases and other state offenders who committed a crime in Telangana for ensuring effective periodic checking management. Also, generate reports on GPS enabled Beat

Management and point book visiting and sharing the information with the concerned officers for understanding the gaps and improving visible policing

- Preparation of area-wise crime history reports for directed patrolling and actionable intelligence
- Analysing effectiveness of Measures taken to eliminate root causes on a periodic basic
- Preparing Traffic incidents reports and analyse whether traffic violations are increasing or decreasing despite booking cases on speed violation, signal jumping, drunken driving etc.
- Preparation of reports / thematic maps to analyse accident-prone areas and to take preventive measures and reengineering with the help of other stakeholders
- Preparation of reports on geo-tagged landmarks for traffic planning and to clear the traffic congestion
- Analysing the data entered in different police applications i.e. CCTNS, TSCOP, HAWKEYE, COP CONNECT, e-petty cases, e-challans etc., and ensuring whether the data entered is accurate and complete
- Guiding the police officers in adhering to the established systems and improving the police functions
- Generating daily, weekly, fortnightly, monthly reports on the nature of crimes & activities and incidents; preserving them in chronological order for easy reference
- Publishing reports on Success Stories involving the effectiveness of various Crime Reduction Strategies adopted by Frontline Police Officers

i) Resources:

The select staff having knowledge in MS Excel, MS PowerPoint, and SQL are to be posted in the Crime Analysis Unit (CAU).

The proposed staff should be drawn from the existing strength of the respective CCRB/DCRB and should work directly under the supervision of Inspector DCRB/CCRB.

Details of proposed strength for managing and working in the Hotspot & Root Cause Analysis Unit are furnished below:

Inspector / SI	HC / PC	support staff	Total
1	3	1	5

Conclusion:

To make the above Centres of Excellence (CoEs) self-reliant, required equipment & tools were purchased and installed at the designated locations in Districts/ Commissionerates of Police. For operationalising and managing the centres, initially select 163 police personnel of various ranks have been trained so far on

'Cybercrime & Cyber Forensics', 'Video Enhancement' and 'Data Analytics' at DGP Office.

i) Process Governance

- Standard Operating Procedures, Templates and training manuals will be maintained by the State IT & C Department. This will be ensuring for updatedness and will be provided periodically to the Centres of Excellence
- Technology requirement shall be addressed through central procurement by the State IT & C Department
- IT and ICT support will be provided to CoEs by the State IT & C Department
- Department officers are requested to adhere to the guidelines set by the State IT & C Department

ii) Standards & Best Practices

All the District / Unit Officers are requested to adhere to the following points to maintain necessary standards and for better functioning of Centres of Excellence (CoEs):

- Creation of a safe and suitable work environment for all the Centres of Excellence
- Provision for uninterrupted power supply with sufficient backup and provision to network all devices
- Adoption of appropriate measures to safeguard the equipment and Software Tools.
- Sensitize the SHO's and other Police Officers on the utility of each Centre of Excellence
- A fortnightly DSR should be sent to the Chief Office on the contribution of each Centre of Excellence in crime investigation
- To keep pace with the latest trends, the concerned officers & staff of the centre of excellence should be encouraged to update their knowledge in relevant fields from time to time for the efficient functioning of the Centres of Excellence
- In respect of the proposed strength for Centres of Excellence, the Police Commissionerates may enhance the proposed strength suitably to cater to the requirements and demand
- DSP rank officer may be nominated as in charge of Command Control Centres located in Commissionerates and Inspector of Police rank Officer for District Command Control Centres

Necessary training to the personnel of all Districts/Units for operationalising the remaining Centres of Excellence will be organised shortly. Hence, all the Unit Officers should identify and nominate suitable candidates who have academic/technical qualifications and have the aptitude to work in the Centres of Excellence.

All the District / Unit Officers are requested to bestow personal interest and take measures to set up the above Centres of Excellence (CoEs) in your respective units and report compliance by 31.08.2019. You should utilize the services of the trained staff at the Centres of Excellence for at least 2 years or till a suitably trained/qualified person is available for performing the duties without dislocation of official work. No incumbent in Centres of Excellence should be transferred without prior approval of the undersigned. The list of trained personnel is enclosed for necessary action.

10/8/2019

Director General of Police
Telangana State, Hyderabad.

To
All the Superintendents of Police / Commissioners of Police
All Range Deputy Inspectors General of Police
The Regional Inspectors General of Police Hyderabad and Warangal

Copy to:

The Addl. Director General of Police, Law & Order, Hyderabad,
The Addl. Director General of Police, Railways, Hyderabad
The Addl. Director General of Police, CID, T.S., Hyderabad.
The Addl. Director General of Police, Technical Services, Hyderabad.
The Director TSPA
All Staff Officers
Police Services Quality Management Unit (PSQMU)
P.S to DGP, TS
The Stock File.

NOTES

NOTES

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

> “Absence of evidence is not evidence of absence”
>
> - Carl Sagan

सत्यमेव जयते
TELANGANA STATE
POLICE
Duty
Honour
Compassion

SOCIAL ENGINEERING CRIMES

CYBER WARRIORS SERIES BOOK-3.0

TELANGANA STATE POLICE