Cybercrimes
SOP

JOGULAMBA GADWAL, CYBERCRIME BRANCH, TELANGANA

Definition

- **Cybercrime is a crime that involves a computer or a network or both.**
  సైబర్ క్రైమ్ అనేది కంప్యూటర్ లేదా నెట్‌వర్క్ లేదా రెండింటినీ కలిగి ఉన్న నేరం.

- **The most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users**
- సైబర్ క్రైమ్ యొక్క ప్రముఖ రూపం గుర్తింపు దొంగతనం, దీనిలో నేరస్థులు ఇతర వినియోగదారుల నుండి వ్యక్తిగత సమాచారాన్ని దొంగిలించడానికి ఇంటర్నెట్‌ను ఉపయోగిస్తారు

- **Accused grab details from victims which may include login information, such as usernames and passwords, phone numbers, addresses, debit/credit card numbers, bank account numbers, and other information criminals can use to "steal“ person's identity. Sometimes accused get all above details on call using social engineering, sometimes they get them using remote access applications while sometimes accused lure users to fake websites, where they are asked to enter personal information.**
- యూజర్ పేర్లు మరియు పాస్‌వర్డ్‌లు, ఫోన్ నంబర్లు, చిరునామాలు, డెబిట్ / క్రెడిట్ కార్డ్ నంబర్లు, బ్యాంక్ అకౌంట్ నంబర్లు మరియు ఇతర సమాచార నేరస్తులు లాగిన్ సమాచారాన్ని కలిగి ఉన్న బాధితుల నుండి నిందితుల వివరాలు వ్యక్తి యొక్క గుర్తింపును "దొంగిలించడానికి" ఉపయోగించవచ్చు. కొన్నిసార్లు నిందితులు అన్నింటినీ పొందుతారు సోషల్ ఇంజనీరింగ్ ఉపయోగించి కాల్‌పై వివరాలు, కొన్నిసార్లు వారు రిమోట్ యాక్సెస్ అనువర్తనాలను ఉపయోగించి వాటిని పొందుతారు, అయితే కొన్నిసార్లు నకిలీ వెబ్‌సైట్‌లకు వినియోగదారులను ఆకర్షిస్తారని ఆరోపించారు, అక్కడ వారు వ్యక్తిగత సమాచారాన్ని నమోదు చేయమని కోరతారు

Method of Investigation

Financial

Most of the Financial fraud done by using mobile. It is required to follow below mentioned details .

1) CDR
2) Bank Statement
3) IPDR log
4) Email Details
5) Wallets Details

Non Financial

- Social Media Requests
- Website Domains
- Email Related

In this type of cases we require the IP Details, Gateway and IPDR details for investigation

Type of Frauds

Sr. No	Fraud Name	Sr. No	Fraud Name
01	OTP/UPI/Google pay link fraud	10	OLX fraud
02	Without OTP Frauds	11	Customer Care Fraud / Helpline Frauds
03	QR code scan Fraud	12	e-Commerce related/ Online shopping Frauds
04	Wallet KYC update fraud	13	Email Related
05	Job fraud	14	Sim swapping Frauds
06	Loan fraud	15	Matrimonial fraud / Gift Frauds
07	Porn Site fraud	16	Lottery/prize Frauds
08	Remote access Fraud	17	Social media
09	Chemical/Seeds related Fraud		

OTP Frauds

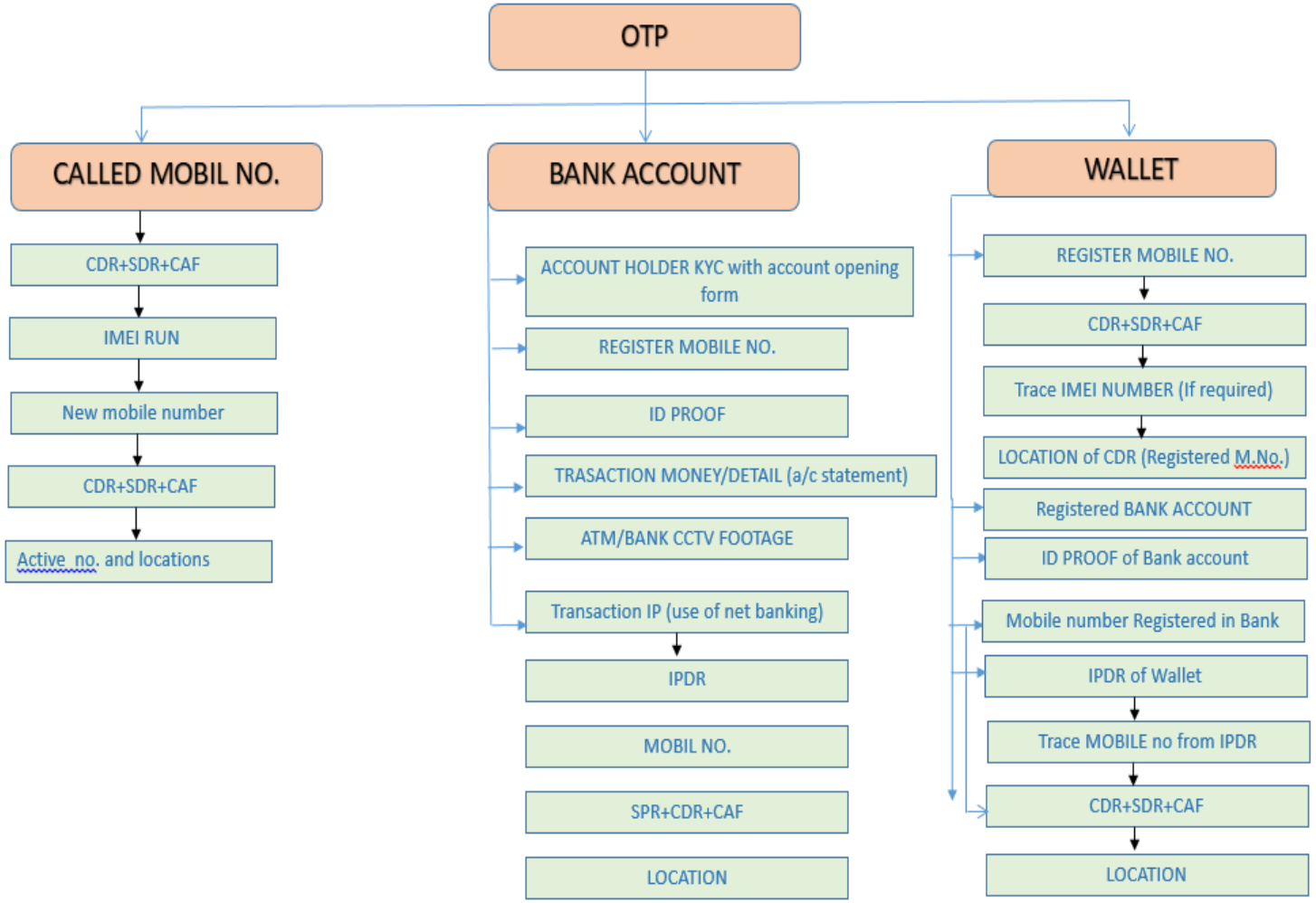
Modus Operandi:-

- AIf victims fall ccused call the victims posing as bank employee/Manager and speak about renewing or upgrading their existing debit/credit card for better benefits. నిందితులు బ్యాంక్ ఉద్యోగి / మేనేజర్‌గా నటిస్తున్న బాధితులను పిలిచి, మెరుగైన ప్రయోజనాల కోసం వారి ప్రస్తుత డెబిట్ / క్రెడిట్ కార్డును పునరుద్ధరించడం లేదా అప్‌గ్రేడ్ చేయడం గురించి మాట్లాడతారు.
- for it then they ask for the debit/credit card number, Card Verification Value, expiry date of the existing card as a part of the upgrade process. After that they ask for the OTP which received in mobile banking number. In this way they transfer amount from victim's bank account. బాధితులు దాని కోసం పడితే, వారు అప్‌గ్రేడ్ ప్రక్రియలో భాగంగా డెబిట్ / క్రెడిట్ కార్డ్ నంబర్, కార్డ్ వెరిఫికేషన్ వాల్యూ, ప్రస్తుత కార్డు యొక్క గడువు తేదీని అడుగుతారు. ఆ తరువాత వారు మొబైల్ బ్యాంకింగ్ నంబర్‌లో అందుకున్న OTP ని అడుగుతారు. ఈ విధంగా వారు బాధితుడి బ్యాం

Proofs required from victims :-

- Bank Details of victim
- Mobile numbers of accused

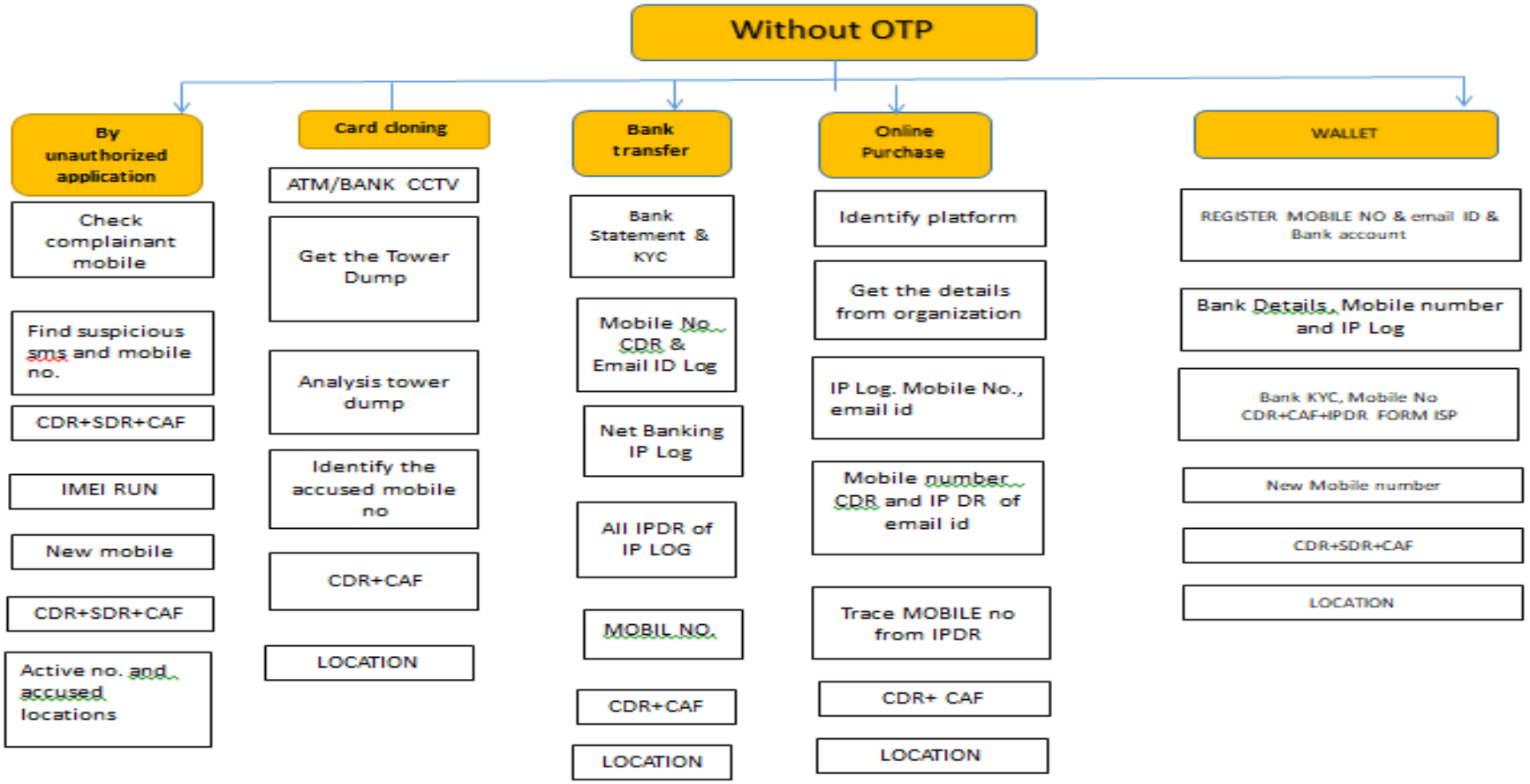
Investigation Flow-chart



Suggested Acts:

- IPC Section 406,419,420,120(B) and IT Act Section 66(C,D)

Without OTP Frauds Investigation Flow-chart



Suggested Acts:

- IPC Section 406,419,420,120(B) and IT Act Section 66(C,D)

QR code scan Fraud

Modus Operandi:-

- Paytm, Phone Pay, Google Pay, Bhim App, Mobikwik, MI Pay, Pay Zaap, Razor Pay Application use QR code scanning for money transfers.
- All the above applications provide QR Code Scan Facility for Money Transfers.
- How to work QR Code: You can pay using your mobile phone by simply scanning the code.
- What is a QR Code: QR stands for quick response and is a type of barcode that can be read using an app and the camera on your smartphone or tablet. A QR code stores information related to the item it's found on. A QR code is basically a two-dimensional type of barcode that can store information in an encoded format. QR code payment is enabled through a smartphone, using which, a customer can scan a QR code to make a payment to any merchant outlet or online stores, etc. After scanning the QR code, the customer will have to key in the transaction amount. After this, the bank account of the user is debited and the merchant is paid directly.
- After scan QR code the victim are asked to write pin numbers, by that the money is transferred into accused wallet account instead of victim’s account.

QR code scan Fraud

- **Step 1:** Go To Settings > Payments. There you will see an option for New Payment
- **Step 2:** Click on New Payments and you will see two options, Pay with UPI ID and Scan OR code. Tap on QR code to scan and enter the desired amount.
- **Step 3:** Once the scan is complete, the app will ask you for the UPI PIN. Enter the PIN and your payment will be successful. The amount will be deducted from the bank account and it will reach the chosen contact's account.
- When you scan a QR Code using your smartphone, you get an immediate access to its content
- An accused gets shop/restaurant contact number from Facebook, Instagram or any website.
- An accused calls the shop/restaurant to purchase their product/food and the accused sends QR code to the shop/restaurant owner to make payment online.
- Because the accused sends the QR code in which payment has to be made and not to be received.
- When the owner scans QR code, his money is transferred to the account of the accused.

Proofs required from victims :-

- Link of fake website, Instagram and/or Facebook
- Mobile numbers of accused
- Collect transaction screenshots and bank statement

Wallet KYC update Fraud

Modus Operandi:-

- Accused call or SMS to victim for update their wallet KYC for uninterrupted wallet service.
- For that the accused send a link to the victim and tell the victim to click the link and install the application. This application may be like Team Viewer, quick support, Any-Desk, etc.
- The accused tell the victim to make transaction of very small amount to update KYC and when victim do this transaction, the accused can see everything.
- The accused gets id/address of this application from the victim and creates a wallet account using victim's mobile number and links victim's bank account with it. Then the accused transfers the money from the victim's bank account to his/her wallet/bank account.

Proofs required from victims :-

- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available

Job Fraud

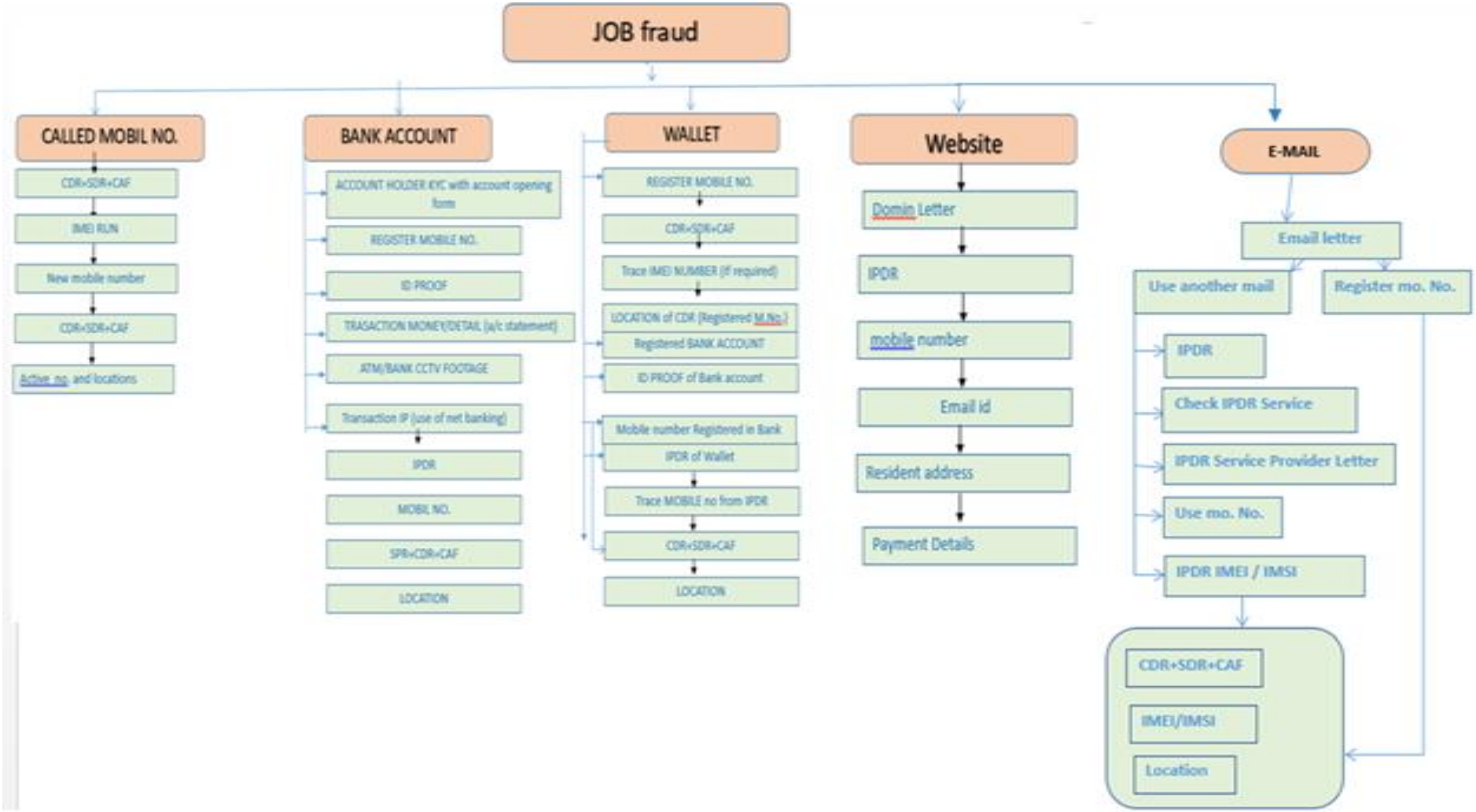
Modus Operandi:-

- An accused gets victim's details from any job registration website.
- The accused calls the victim and tells that they are from xxxjobs.com and ask about field of interest and location for job.
- As per the victim's interest, they convince the victim for online registration.
- Victims fill up the form and submit debit card details in phishing page using which accused transfers the money from victim's bank account, after that in the name of different file processing fees and refund of debited amount the fraud is committed.

Proofs required from victims :-

- Fake Website Link
- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available
- Email id of the accused

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120 (B) IT Act Section 66(C,D)

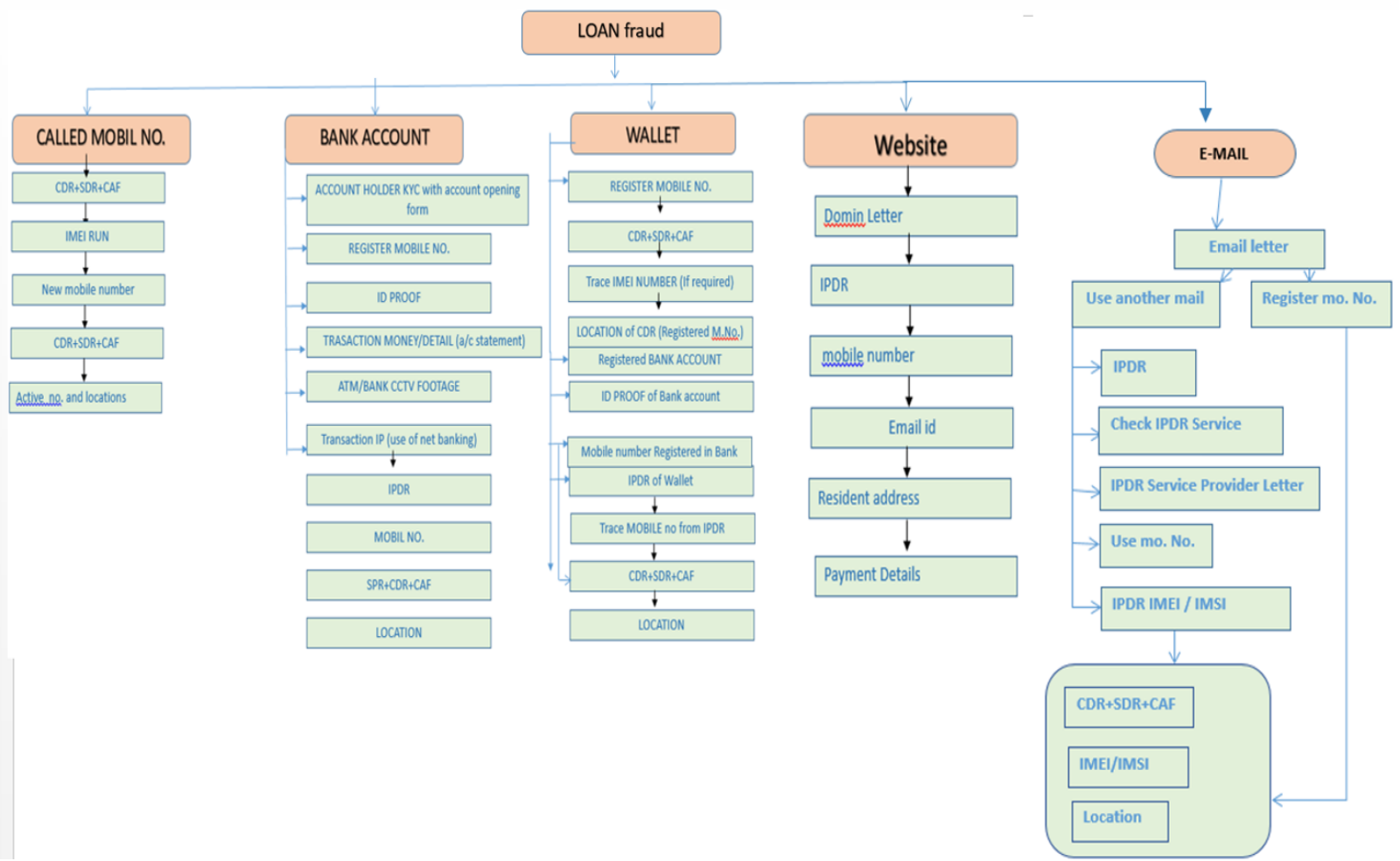
Loan Fraud

- Victims search on Google for loan and upload their biodata on various websites like mudra loan, optimum services etc.
- Some times victims get SMS or direct phone calls for Loan.
- Some Times victims get newspaper Ads for low interest loan.
- Accused calls the victims and sends E-mail for approving his loan, in the guise of officers of reputed banks, Financial Institution (FI). They tell the victim that he is eligible for special, low interest loan.
- Ask for soft copy of your ID, Address Proof, PAN, Bank A/C Details, copy of cancelled cheque, Pay slip, income details, ITR online on WhatsApp or email.
- Then they send the loan application form.
- Then the accused sends the loan approval letter and ask you to pay file charges, refundable security, processing fee

Proofs required from victims :-

- Fake Website Link and email address of accused
- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120 (B) IT Act Section 66(C,D)

Porn Site Fraud

Modus Operandi:-

- Accused put photographs and mobile numbers of victim and his/her family members on porn websites.
- When victims tell to remove them, accused ask for money.
- Sometimes Accused put morphed photographs or videos along with mobile numbers of the victim.

Proofs required from victims :-

- Link of porn website
- Mobile number of accused
- Collect transaction screenshots and bank statement

Chemical/Seeds related Fraud

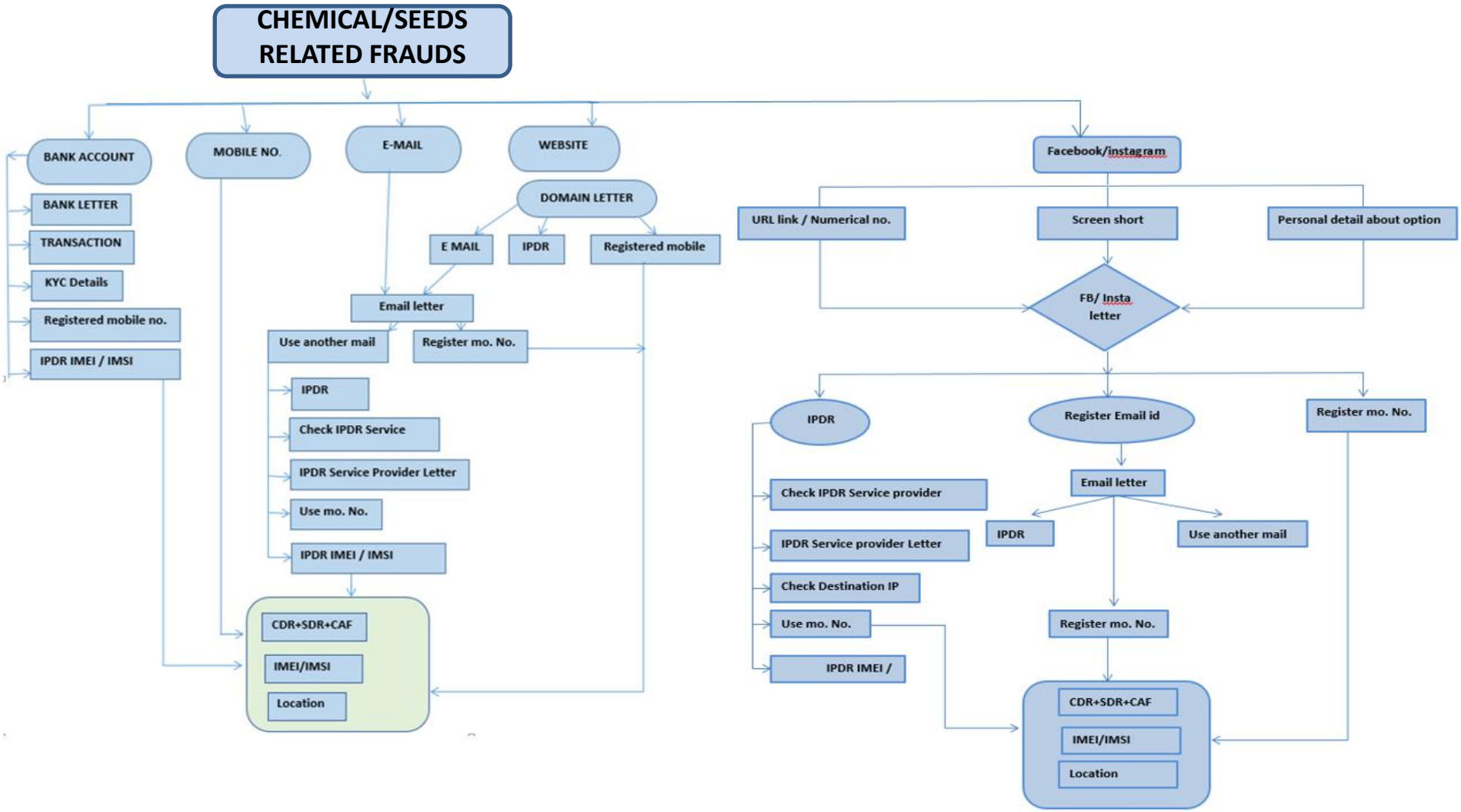
Fraud details :-

- An accused (A-1) makes friendship with the victim on social media and chat about the business of cancer medicine/seeds using foreign/virtual number. Also tells that they need raw material for research.
- Victim purchases medicine/seeds as a raw material paying in advance to the raw material provider accused (A-2). The accused says to the victim that he sent this sample material to foreign country for testing and says that the sample is approved.
- Then accused asks for large quantity and so the victim purchases raw material by paying a huge amount. Once full payment is made the accused never pick up victim's phone and never reply on social media.

Proofs required from victims :-

- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available
- Email id, facebook id and link of accused

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120(B), IT Act Section 66(C)

OLX Fraud

Modus Operandi:-

- Criminals make fake profiles on OLX and they get photos of product and vehicle from OLX profiles of other people and put these photos for selling at lower price on fake OLX profile.
- They collect vehicle's/product's documents like RC book, insurance policy, mobile purchase bill, etc from the original seller.
- Interested people calls on the number given in fake OLX profile.
- Criminals use identities of Defence or CAPF officers and say that they get all these things cheaper from army canteen and send fake ID cards or Army canteen cards to victim to gain their confidence.
- They ask the victims for money as transportation charge in advance.
- After getting money they call using another number that your vehicle has arrived but there is a ban on your vehicle and you must pay to release your vehicle and victims pay them.

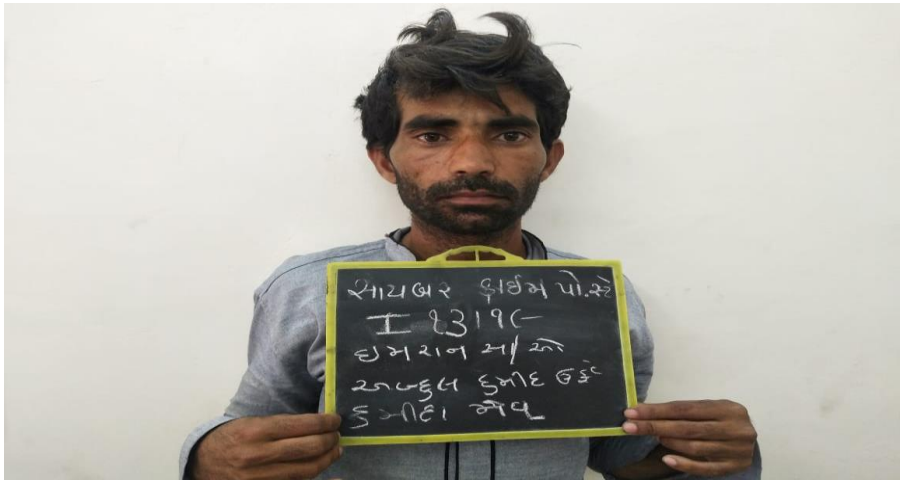
- After getting money they blocks victim's number or never pick up victim's phone and vehicle never reach to the victim's destination.

Fake ID Card

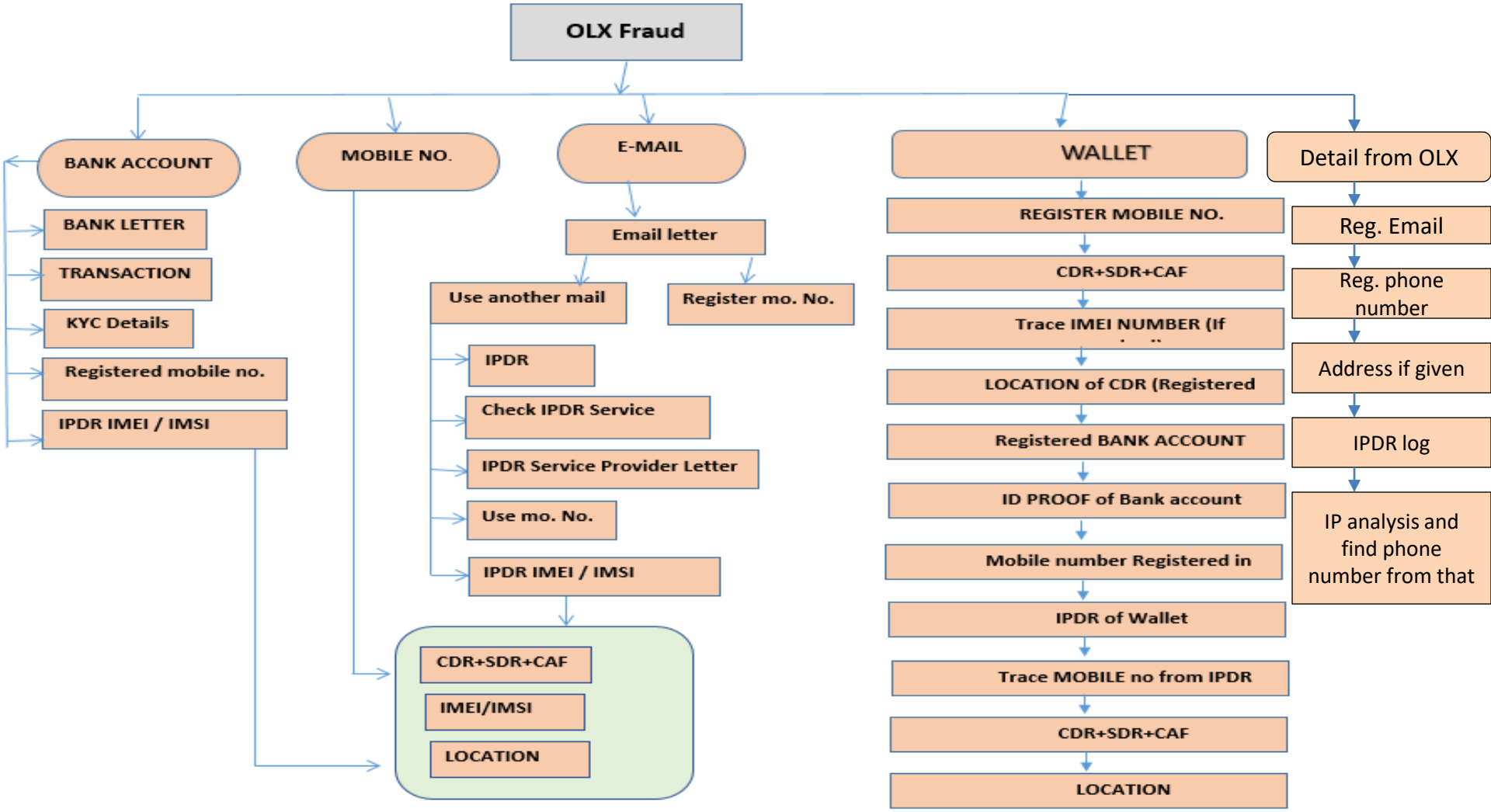
Fake Photo

Proofs required from victims :-

- Fake OLX profile
- Mobile numbers of accused
- Fake ID proof of Army officer
- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available



Investigation Flow-chart



Suggested acts:

- IPC Section 419, 420,465,468 IT Act Section 66(C)

Customer Care Fraud

Modus Operandi:-

- Fraudsters create google business listing page in the name of any known brand/helpline and put their contact numbers.
- Criminals use Google SEO (Search Engine Optimization) to do the jugglery.
- Citizens search for customer care number especially of e-Wallet companies, when they find any issue with application.
- Then the victims fall in the trap of cyber criminals, who pretend to be the real customer care center, take all the details from the victim and the citizen becomes a victim of their fraud.

Proofs required from victims :-

- Copy of bank account statement of victim
- Google Fake listing screenshots and links
- Mobile numbers of accused
- Screenshots of debit messages if available

Helpline Fraud

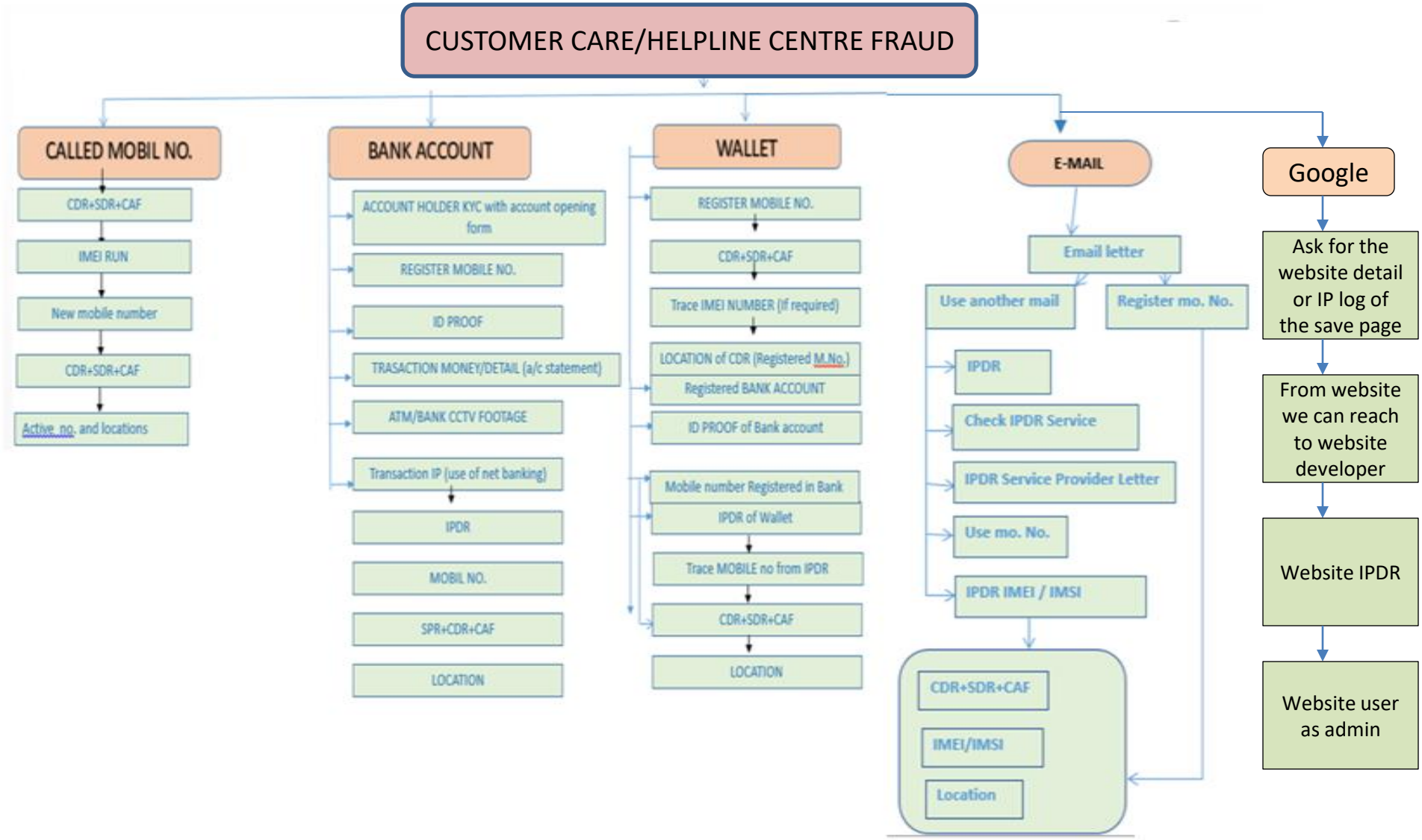
Modus Operandi:-

- Same as Customer Care fraud, when victims use Google search for any helpline like Animal care, Health care, Bank Helpline, hotel booking etc., they find the numbers of the cyber criminals on very first page on Google.
- Victims call on these numbers to get help and victimized.
- Citizens call on the topmost number to get help in their problems like getting refund, get information about company, book a room/table in a hotel, help animals/birds, etc.
- The Fraudsters ask the citizens for bank account details for refund, booking a room/table in a hotel, helping animals/birds and the Fraudsters transfer the funds in their own accounts.
- Criminals ask the victims to pay some minimum amount like 10Rs to verify and start the service, send the UPI link and get amount like 10000 to 50000Rs.

Proofs required from victims :-

- Copy of bank account statement of victim
- Google Fake listing screenshots and links
- Mobile numbers of accused
- Screenshots of debit messages if available

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120(B), IT Act Section 66(C,D)

e-Commerce related Fraud

Modus Operandi:-

- Victim cancels order for which he/she already paid online
- An accused gets victim's contact number from that e-Commerce company
- An accused calls the victim to refund money and gives a link to the victim and says to fill up a form.
- The victim fills up the form and submit debit/credit card details in phishing page through which accused transfers victim's money in his bank account or purchase something using victim's money.

Investigation:- Same as OLX Fraud and Credit Card Fraud.

Proofs required from victims :-

- Fake Website Link
- Invoice Copy of order and delivery
- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available

Online shopping Fraud

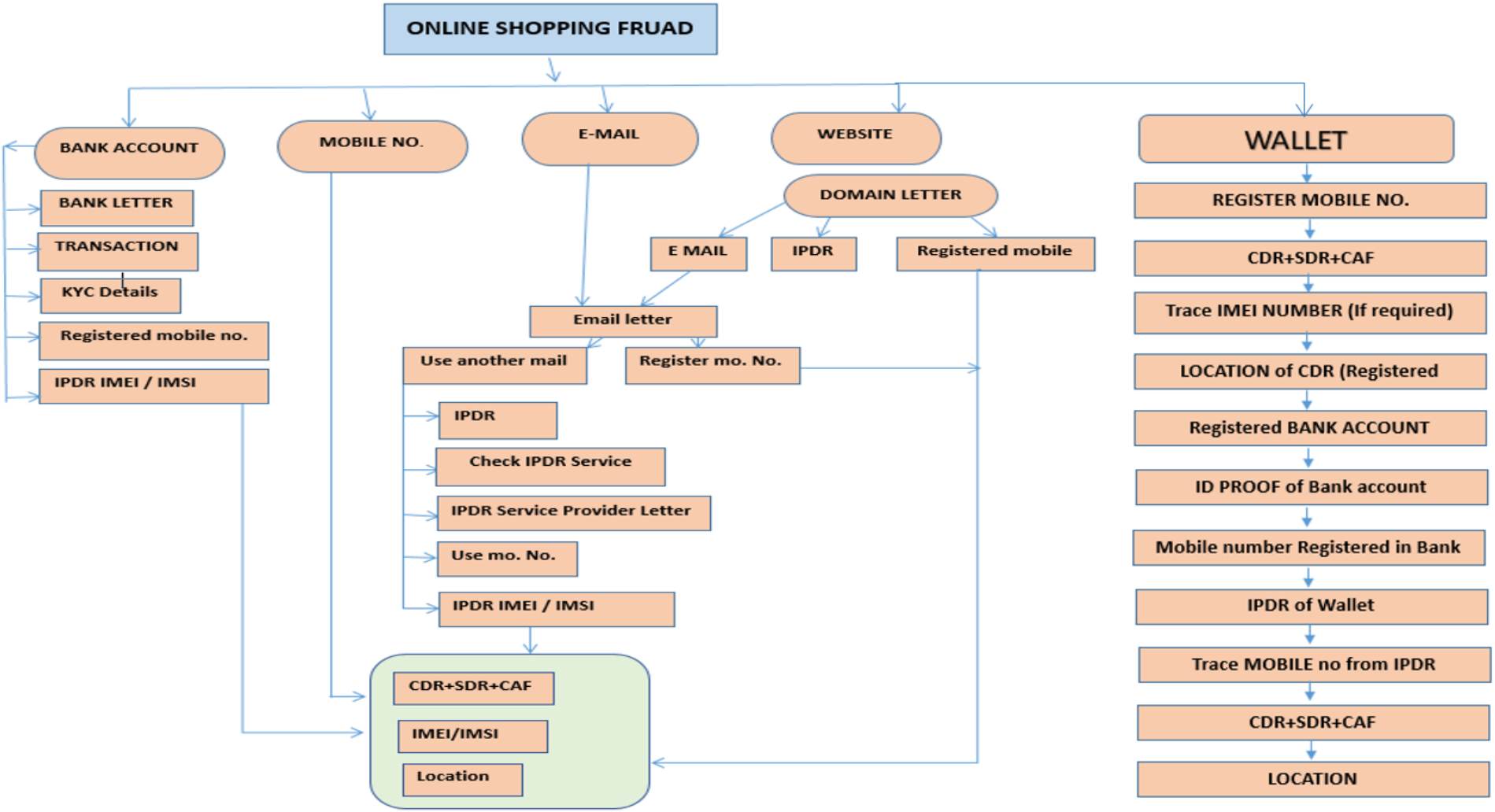
Modus Operandi:-

- An accused create a fake website and puts the products for selling for lower prices on this website.
- Victim shows the interest in purchasing any of the product and makes online payment
- The victim never gets the product and loses money.

Proofs required from victims :-

- Link of fake website
- Mobile number of accused
- Invoice copy and delivery receipt of shopping if available
- Collect transaction screenshots and bank statement

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120 (B) IT Act Section 66(C,D)

Email Related Crimes

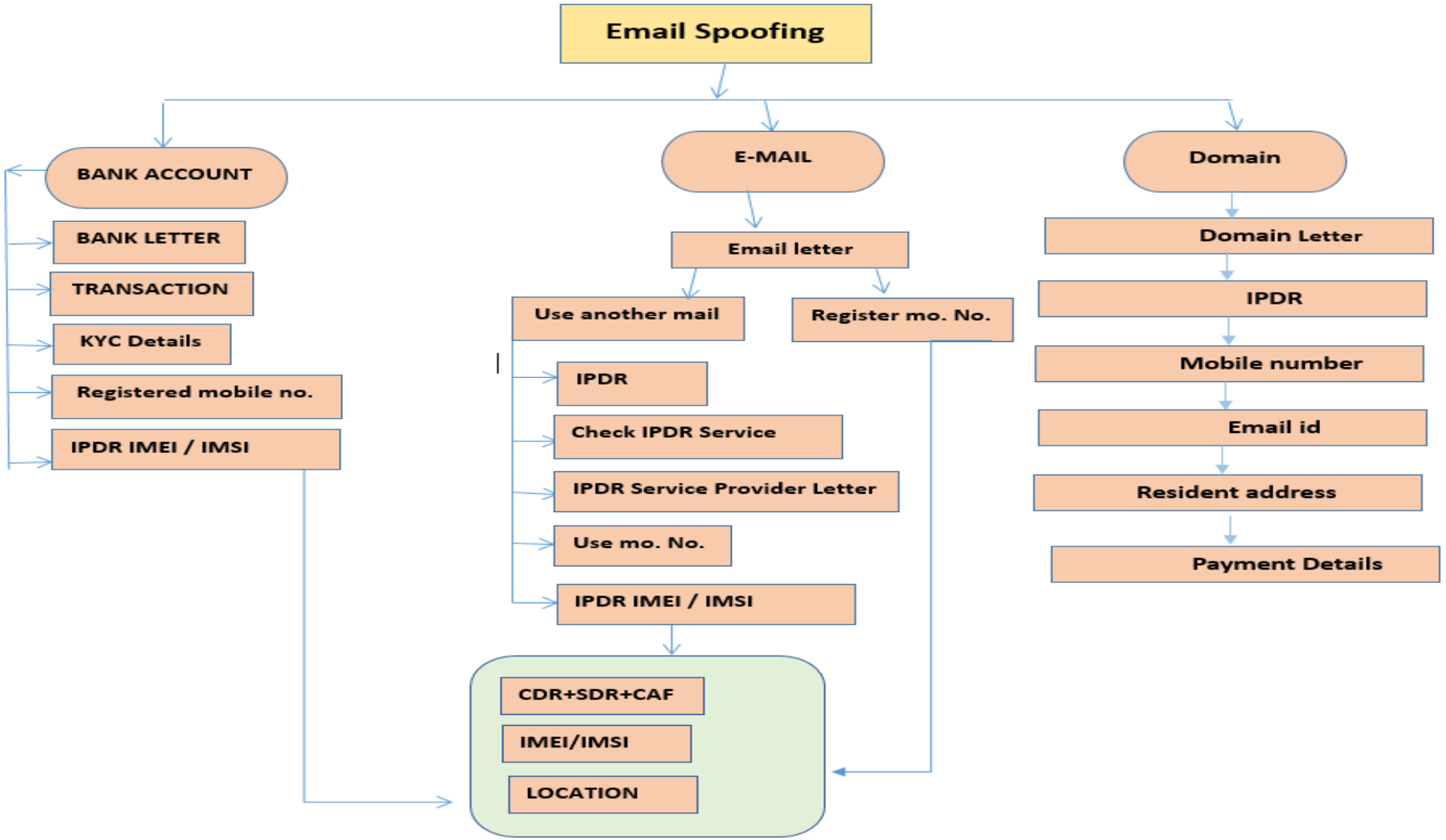
Types:

- Email spoofing: Accused do chatting with victims about business deals using email ids of same company name. They create new fake email id in the name of company and send email with changed bank details and instruct to send their future payments in these bank accounts. So victims transfer huge amount in the bank accounts of the accused for business deals.
- Email hacking: In this crime, a hacker illegally gains access to a laptop/ desktop/ tablet. The hacker sends an email or a link to the victim in social media/ online platform. Once the victim opens it, with help of specialized software the hackers can steal details such as bank passwords, transaction details and email conversations.
- Defamation by email: Accused publish material giving false information about victims, their business or their families on social media platforms. This material is harmful to the reputation of the victims, their business or their family.
- Sharing obscene material by email: Accused share nude photos, nude videos to victims and ask for money by threatening them publishing in social media platforms, websites or on YouTube channels.

Proofs required from victims :-

-Email message
-Email ID (similar @ fake)
-Bank statement of victim

Investigation Flow-chart



Suggested acts:

- IPC Section 420, 465,467, 468, 471 IT Act Section 66(C,D), 65

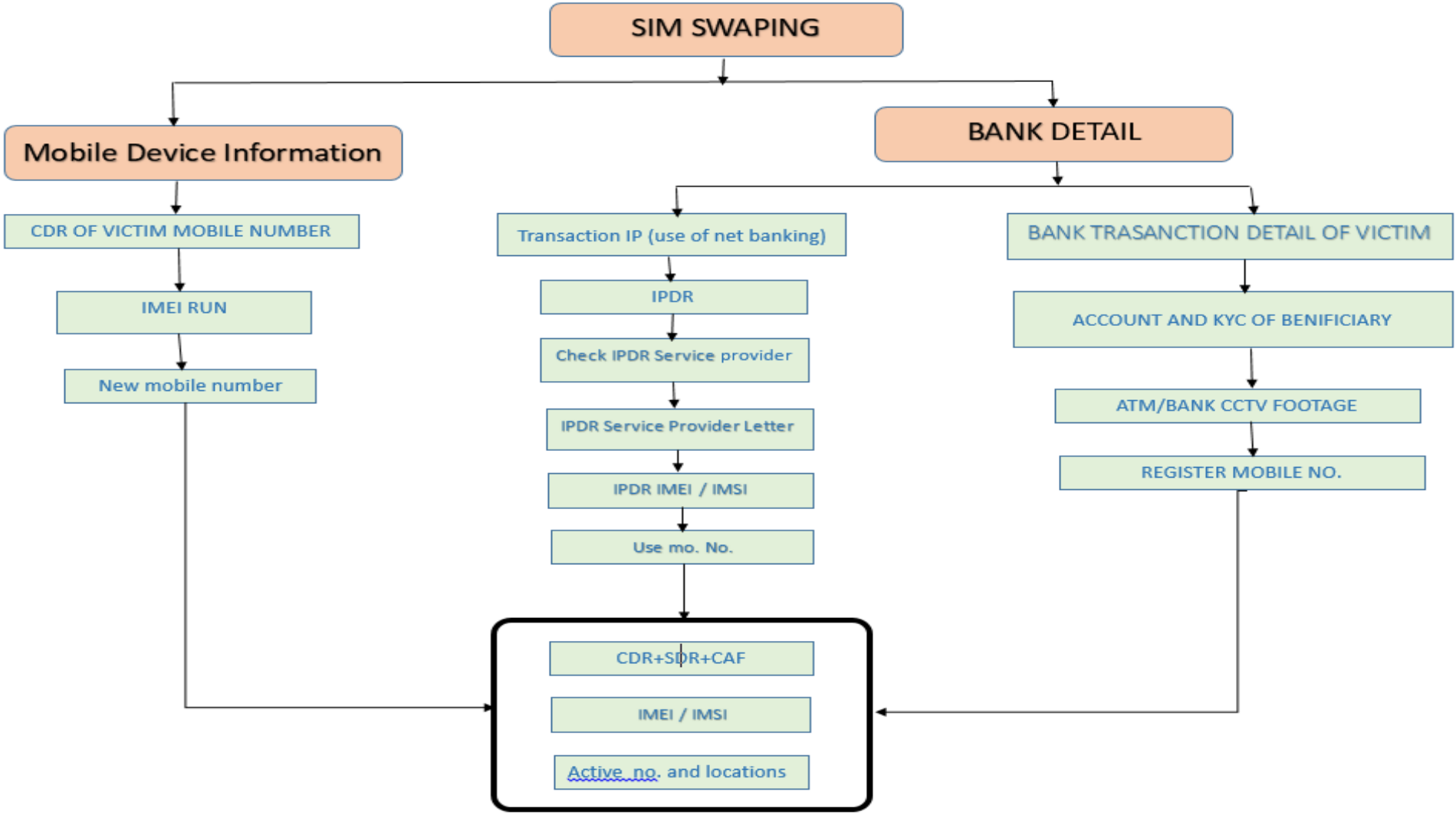
Sim swapping Fraud

- A Fraudster gathers details about the victim contact, his personal information, the victim's mobile service provider, etc.
- The Fraudster uses social engineering techniques and the details about the victim to convince the service provider to port the victim's phone number to the Fraudster's SIM.
- They call the MSP impersonating the victim. They get a new SIM activated. This ports the victim’s number to the accused’s device with a new SIM.
- Once this happens the victim's phone loses connection to the network and the Fraudster will receive all the SMS and voice calls intended for the victim.
- This allows the Fraudster to intercept any One Time Passwords sent via SMS or telephone calls to the victim. So victim does not get any OTP messages and accused transfers huge amount through net banking to different bank accounts from victim's bank account.
- The accused may also transfer money to a new account in your name at your bank, where because you are already a Bank Customer, there may be less robust security checks.
- Transfers between those two accounts in victims name might not sound any alarm.
- <u>SIGNS:</u>
    - You are not able to place calls or text.
    - You are notified of activity elsewhere.
    - You are unable to access accounts.

Proofs required from victims :-

- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available
- Registered mobile number for Net banking

Investigation Flow-chart



Suggested acts:

- IPC Section 420,465,467, 120(B),IT Act Section 66(C),66D)

Matrimonial/Gift Fraud

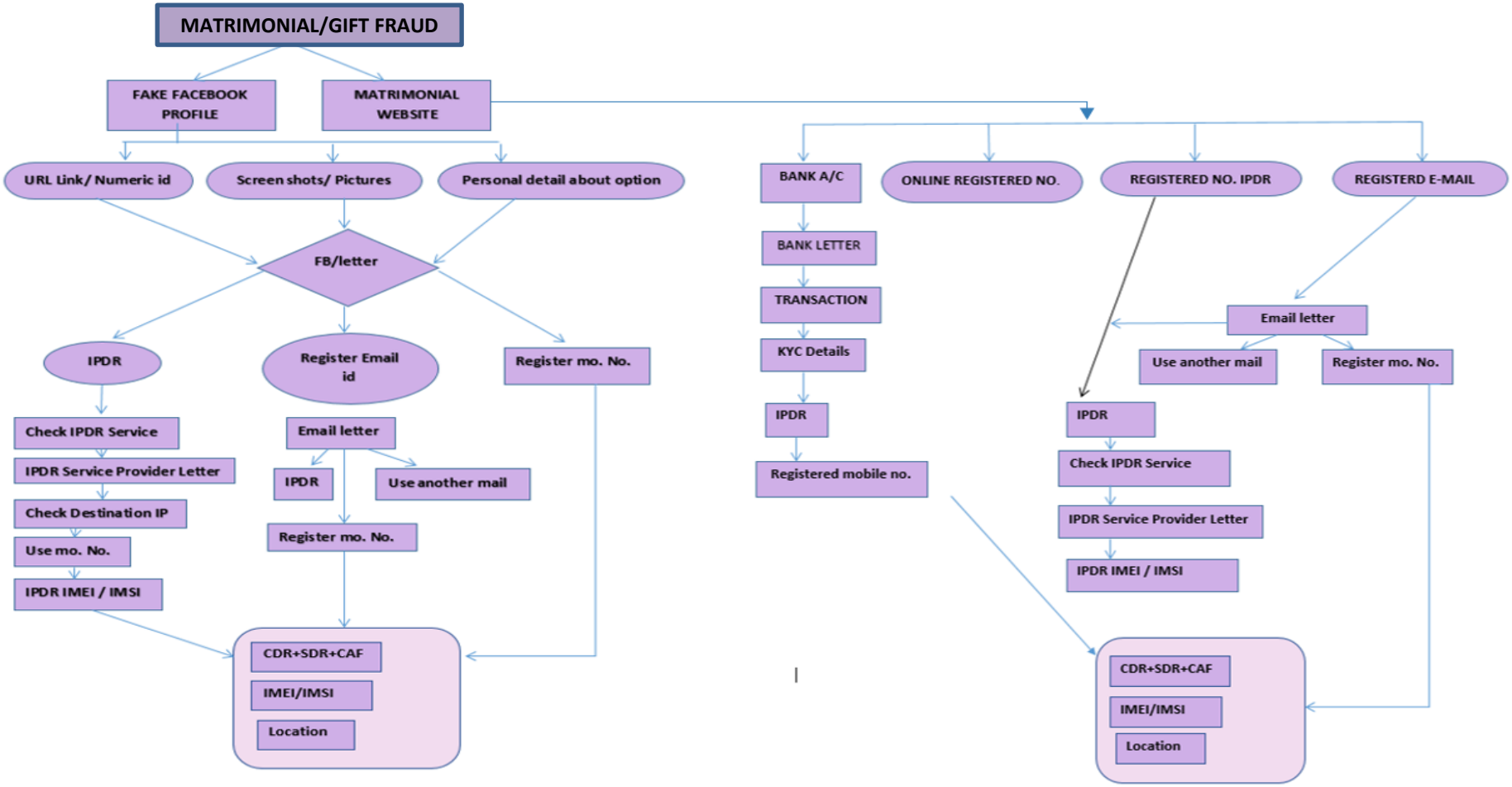
Fraud details :-

- Gift fraud is same as above, after generating faith on social media. Criminals claimed that they have sent a gift from foreign to victim.
- Then victim gets fake calls from customs or other department to pay the duty, processing fees etc.
- Victim also gets threating calls for legal consequences. Large amounts are thus paid by the victim for the gift that he never gets.
- Identified the Matrimonial website or any other way on which complainant has communicated with fraud person.
- Get the Mobile Number, Email ID, User name of the fraud person from complainant which he has been cheated.
- Way of transfer money to fraud person account.
- Identified the BANK, E wallet, Money Transfer Company , UPI Service or any other way.

Proofs required from victims :-

- Copy of bank account statement of victim
- Mobile numbers of accused
- Screenshots of debit messages if available
- Email id, facebook id and link of accused

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120(B), IT Act Section 66(C,D)

Lottery/prize Fraud

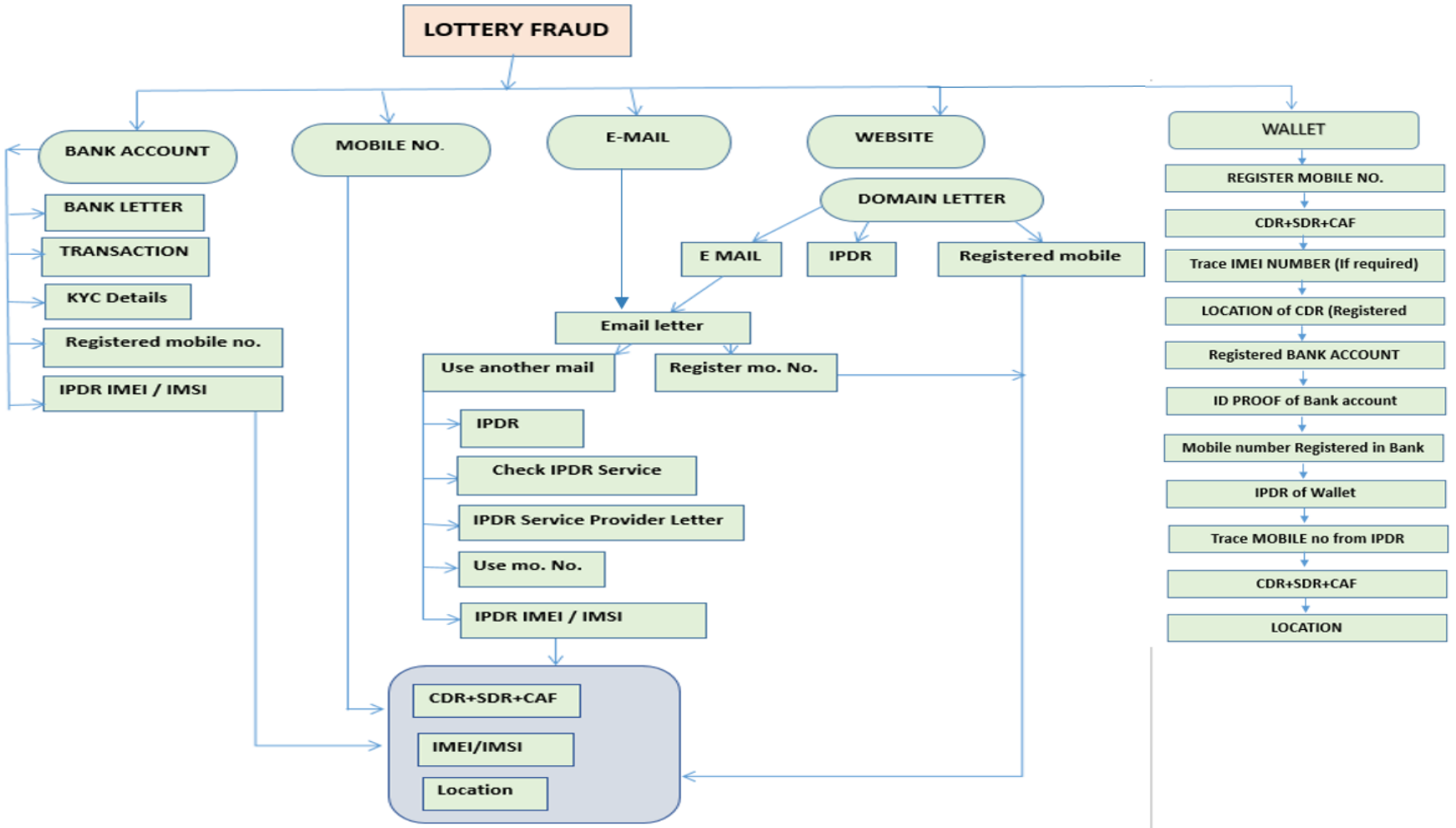
Modus Operandi:-

- In this type victims purchases products online with surety of gift on shopping of any product from website.
- After some days victims receive call from the same website and get to know that he wins a gift prize.
- In the name of different processing fees the accused tells the victims to transfer some amount to bank/wallet account of accused.

Proofs required from victims :-

- Invoice copy and delivery receipt of shopping if available
- Mobile number of accused
- If victim made payment to the accused then collect payment link screenshots

Investigation Flow-chart



Suggested acts:

- IPC Section 406, 420, 120(B), IT Act Section 66(C,D)

Social Media related Frauds

- Identity theft: **Identity theft** is the crime of obtaining the personal or financial information of another person for the purpose of assuming that person's name or **identity** to make transactions or purchases.

గుర్తింపు దొంగతనం: లావాదేవీలు లేదా కొనుగోళ్లు చేయడానికి ఆ వ్యక్తి పేరు లేదా గుర్తింపును of హించుకునే ఉద్దేశ్యంతో మరొక వ్యక్తి యొక్క వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని పొందడం నేరం.

- Fake identity: Fake identity is the fake information with actual ID data. For example, combining a real aadhar number along with a fake address. The fraudster can then use the fake identity to acquire sim cards, passports and other real ID as well as to open bank accounts or to get credit cards.

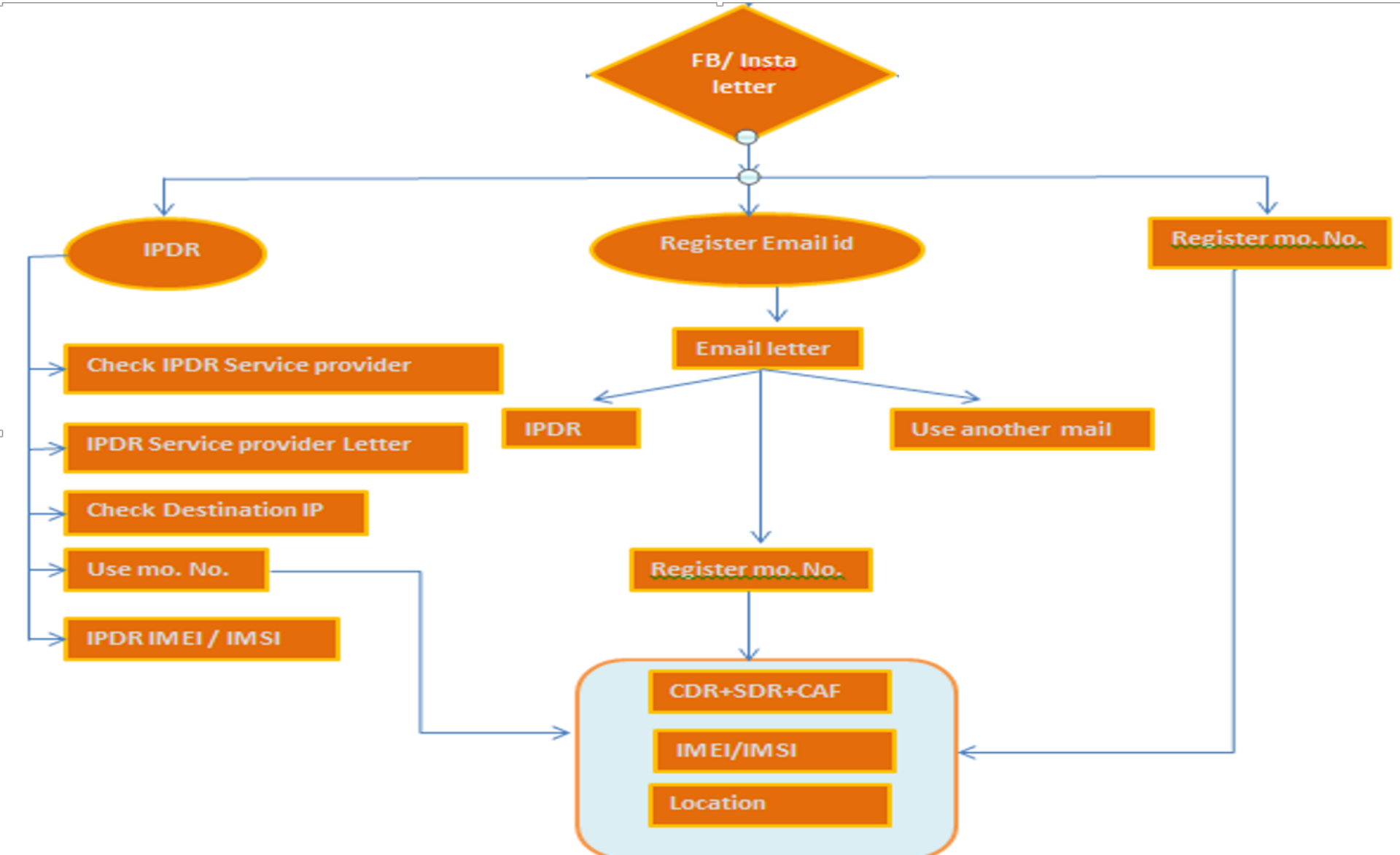
నకిలీ గుర్తింపు: వాస్తవ ఐడి డేటాతో నకిలీ సమాచారం నకిలీ గుర్తింపు. ఉదాహరణకు, నిజమైన ఆధార్ నంబర్‌తో పాటు నకిలీ చిరునామాను కలపడం. మోసగాడు అప్పుడు సిమ్ కార్డులు, పాస్‌పోర్ట్‌లు మరియు ఇతర రియల్ ఐడిని సంపాదించడానికి అలాగే బ్యాంక్ ఖాతాలను తెరవడానికి లేదా క్రెడిట్ కార్డులను పొందటానికి నకిలీ గుర్తింపును ఉపయోగించవచ్చు.

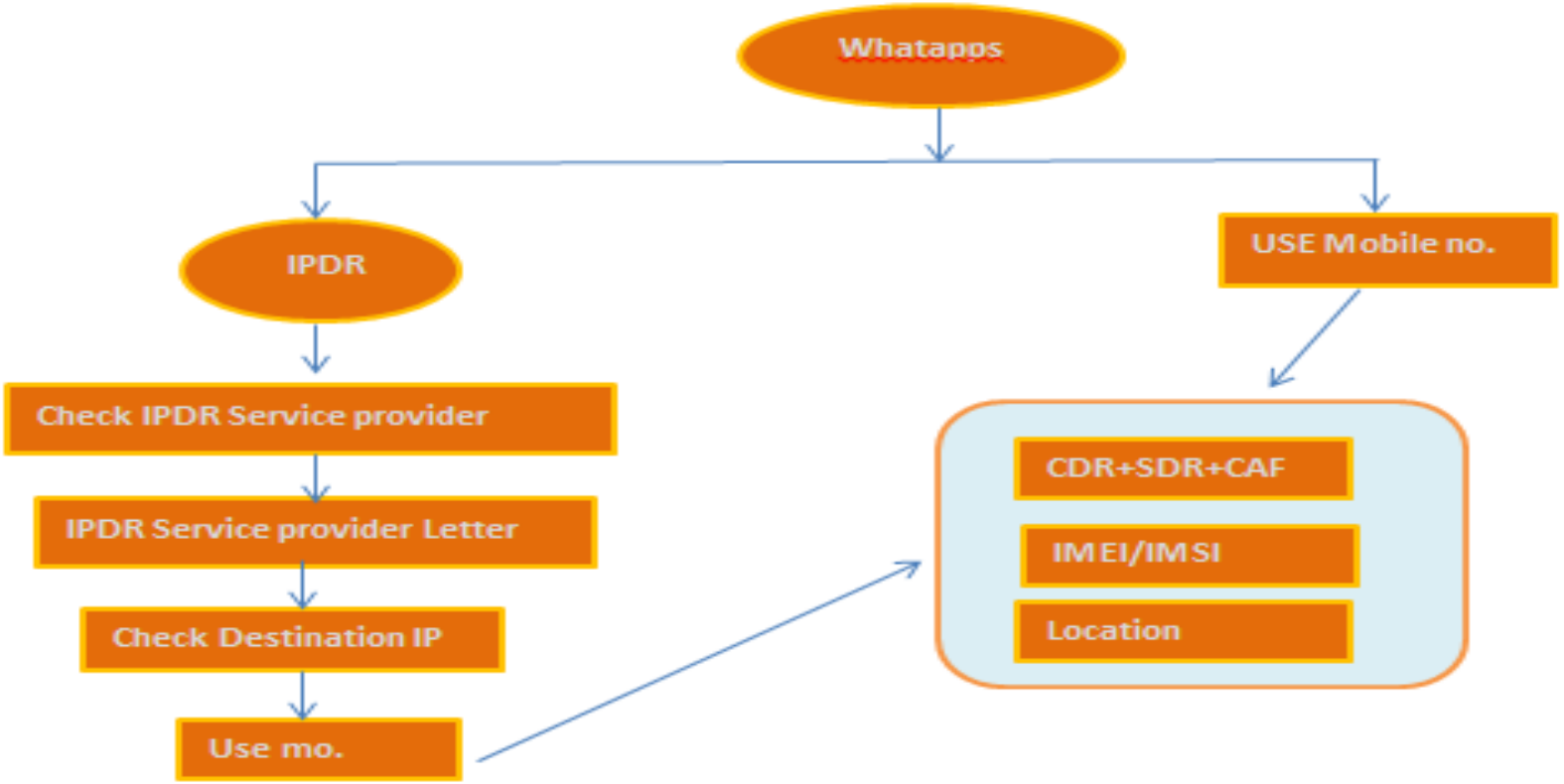
- Sharing obscene material or sexual content by FB, Instagram, email, whatsapp, etc.

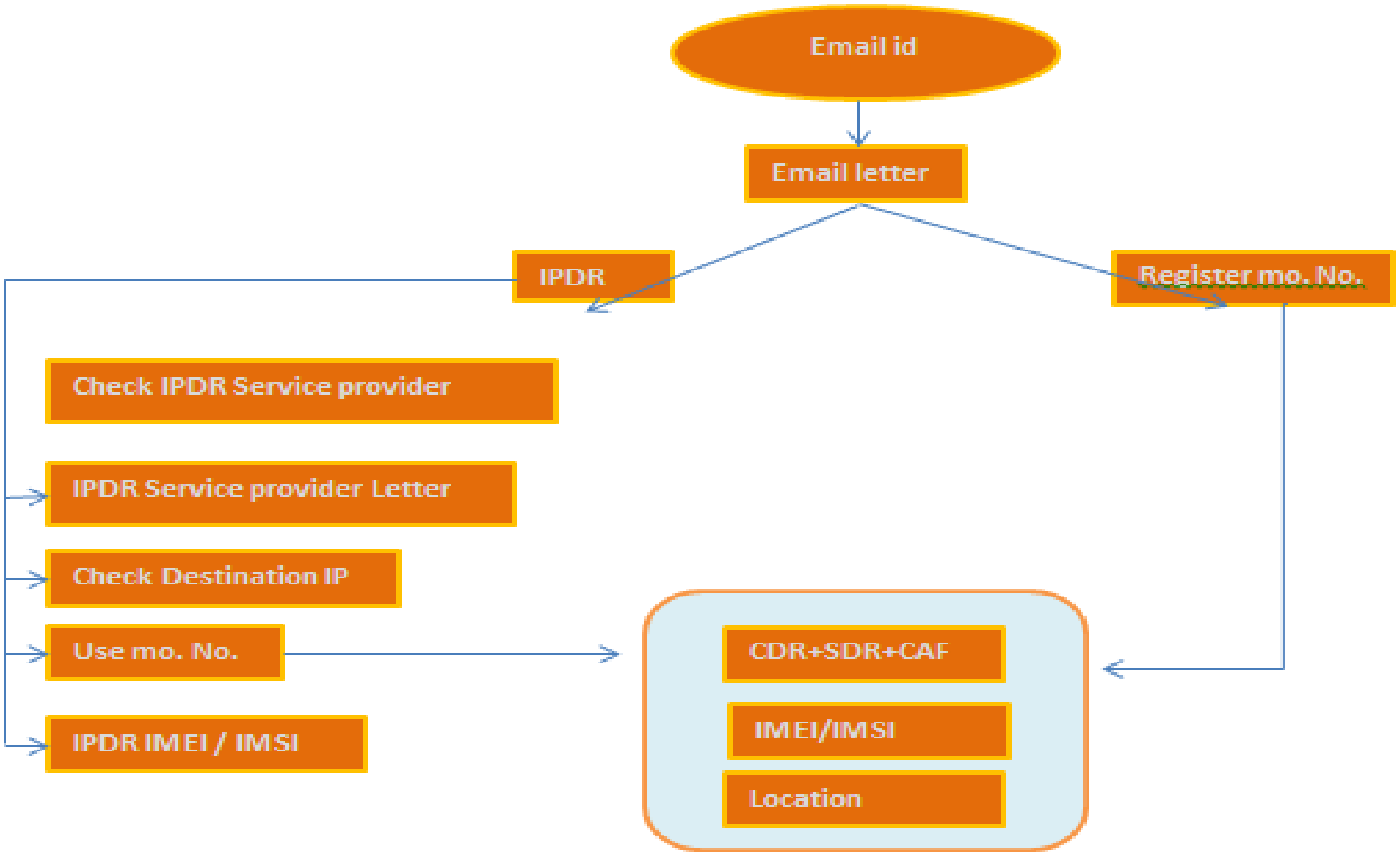
FB, Instagram, email, whatsapp మొదలైన వాటి ద్వారా అశ్లీల పదార్థం లేదా లైంగిక కంటెంట్‌ను పంచుకోవడం.

- Child pornography: Child pornography is any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old). Images of child pornography are also referred to as child sexual abuse images.

చైల్డ్ అశ్లీలత: చైల్డ్ అశ్లీలత అనేది మైనర్ (18 సంవత్సరాల కంటే తక్కువ వయస్సు ఉన్న వ్యక్తులు) పాల్గొన్న లైంగిక అసభ్య ప్రవర్తన యొక్క దృశ్యమాన వర్ణన. పిల్లల అశ్లీల చిత్రాలను పిల్లల లైంగిక వేధింపుల చిత్రాలుగా కూడా సూచిస్తారు.


FB/ Insta letter
IPDR
Register Email id
Register mo. No.
Check IPDR Service provider
IPDR Service provider Letter
Check Destination IP
Use mo. No.
IPDR IMEI / IMSI
Email letter
IPDR
Use another mail
Register mo. No.
CDR+SDR+CAF
IMEI/IMSI
Location


Whatapps
IPDR
USE Mobile no.
Check IPDR Service provider
IPDR Service provider Letter
Check Destination IP
Use mo.
CDR+SDR+CAF
IMEI/IMSI
Location


Email id
Email letter
IPDR
Register mo. No.
Check IPDR Service provider
IPDR Service provider Letter
Check Destination IP
Use mo. No.
IPDR IMEI / IMSI
CDR+SDR+CAF
IMEI/IMSI
Location

Method of Investigation for all Cybercrime

- Take the CDR, SDR and CAF of Mobile Number mentioned in the complaint and ask for the domain details. Also ask for IP details, registered email address and registered mobile number of the fraud website.
- Trace IMEI of deactivated number and get new active numbers, again take CDR of the same activated numbers.
- Do IP analysis and get a number registered with Fraud website.
- Trace the probable locations of accused by analysis of all CDR and mobile device information
- Analyze the transactions details of accuse wallet, bank account where money was deposited by victim.
- By above all factors analysis you may identify an accused.
- Remember every digital trace puts IP log at every step.
- All websites or platforms are keeping basic details of the users. These details can always lead us for detections.

IT act 2008

Section	Offence	Short Description	Classification of Offence
43	Penalty and compensation for damage to computer, computer system	-	Definition
65	Tampering with computer source Documents	Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network.	Imprisonment up to three years, or/and with fine up to ₹2 Lac Cognizable— Bail able
66	Computer Related offences	If Any person dishonestly ,or fraudulently does any act referred to in Section 43.	Imprisonment up to three years, or/and with fine up to ₹5 Lac Cognizable— Bailable
66B	Dishonestly receiving stolen computer resource or computer device	Whoever dishonestly receive retains any stolen computer resource or computer device knowing or having reason to believe the same to be stolen	Imprisonment up to three years, or/and with fine up to ₹1 Lac Cognizable— Bailable
66C	Identity theft	Whoever fraudulently or dishonestly make use of the electronic signature, password or any other unique identification features of any other person	Imprisonment up to three years, or/and with fine up to ₹1 Lac Cognizable— Bailable
66D	Cheating by personation by using computer resource	Whoever by means of any communication device or computer resource cheats by personation	Imprisonment up to three years, or/and with fine up to ₹100,000 Cognizable— Bailable
66E	Violence of privacy: Publishing private images of other	Whoever intentionally or knowingly captures, publishes, or transmits the image of a private area of any person	Imprisonment up to three years, or/and with fine up to ₹200,000 Cognizable— Bailable

IT act 2008

Section	Offence	Short Description	Penalty
66F	Acts of cyber terrorism	With intent to threaten the unity, integrity, security or sovereignty of India. Without authorization Knowingly or intentionally penetrates or accesses computer resources which are restricted for the reasons of the security of the state or foreign relations.	Imprisonment up to life Cognizable— Non Bailable
67	Publishing information which is obscene in electronic form.	Acts\67.png	Imprisonment up to five years, or/and with fine up to ₹1,000,000 Cognizable— Bailable
67A	Publishing images containing sexual acts	Acts\67A.png	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	Acts\67B.png	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Acts\67C.png	Imprisonment up to three years, or/and with fine
68	Failure/refusal to comply with orders	Acts\68.png	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	Acts\69.png	Imprisonment up to seven years and possible fine
70	Securing access or attempting to secure access to a protected system	Acts\70.png	Imprisonment up to ten years, or/and with fine

Indian Penal Code (IPC) 1860

Section	Offence	Penalty	CLASSIFICATION OF OFFENCE
417	Punishment for cheating	Imprisonment of either description for a term which may extend to one year, or with fine, or with both	Non-cognizable—Bailable
420	Cheating and dishonestly inducing delivery of property	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine	Cognizable—Non-bailable
406	criminal breach of trust	Imprisonment up to three years or with fine or with both	Cognizable—Non-bailable
467	Forgery of valuable security, will, etc.	Imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine	Para I- Non-cognizable—Non-bailable Para II- Cognizable—Non-bailable
468	Forgery for purpose of cheating	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine	Cognizable—Non-bailable

Indian Penal Code (IPC) 1860

Section	Offence	Penalty	CLASSIFICATION OF OFFENCE
469	Forgery for purpose of harming reputation	imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.	Cognizable—Bailable
471	Using as genuine a forged document or electronic record	Imprisonment up to ten years, or/and with fine	Cognizable—Bailable

Thank You