

BE(A)WARE



**A BOOKLET
ON
MODUS OPERANDI
OF
FINANCIAL FRAUDSTERS**



RESERVE BANK OF INDIA





Table of Contents

	Subject	Page No.
	<u>Preface</u>	1
	<u>Part A - Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks</u>	2
1	<u>Phishing links</u>	3
2	<u>Vishing calls</u>	4
3	<u>Frauds using online sales platforms</u>	5
4	<u>Frauds due to the use of unknown / unverified mobile apps</u>	6
5	<u>ATM card skimming</u>	7
6	<u>Frauds using screen sharing app / Remote access</u>	8
7	<u>SIM swap / SIM cloning</u>	9
8	<u>Frauds by compromising credentials through search engines</u>	10
9	<u>Scam through QR code scan</u>	11
10	<u>Impersonation on social media</u>	12
11	<u>Juice jacking</u>	13
12	<u>Lottery frauds</u>	14
13	<u>Online job frauds</u>	15
14	<u>Money mules</u>	16
	<u>Part B - Modus Operandi and Precautions to be taken against Fraudulent Transactions - NBFCs</u>	17
1	<u>Fake advertisements for grant of loans</u>	18
2	<u>SMS / Email / Instant Messaging / Call scam</u>	19
3	<u>OTP based frauds</u>	20
4	<u>Fake loan websites / App frauds</u>	21
5	<u>Money circulation / Ponzi / Multi-Level Marketing (MLM) scheme frauds</u>	22
6	<u>Loans with forged documents</u>	23
	<u>Part C - General precautions to be taken for financial transactions</u>	24
	<u>Glossary</u>	32



Preface

There has been a surge in usage of digital modes of payment in the recent years. This gained further momentum during the Covid-19 induced lockdowns. While enhancing customer convenience, it also furthered the national objective of financial inclusion. However, as the speed and ease of doing financial transactions has improved, the number of frauds reported in retail financial transactions have also gone up. Fraudsters have been using innovative methods to defraud the common and gullible people of their hard-earned money, especially the new entrants in the use of digital platforms who are not entirely familiar with the techno-financial eco-system.

This booklet has been compiled from various incidents of frauds reported as also from complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are inexperienced, or not so experienced, in digital and electronic modes of financial transactions. The booklet is intended to create awareness among the members of public about the modus operandi adopted by fraudsters to defraud and mislead them, while also informing them about the precautions to be taken while carrying out financial transactions. It emphasizes the need for keeping one's personal information, particularly the financial information, confidential at all times, be-ware of unknown calls / emails / messages, practicing due diligence while performing financial transactions and changing the secure credentials / passwords from time to time. Hence the title **BE(A)WARE** – Be Aware and Beware!

This booklet is part of the public awareness initiative by the Consumer Education and Protection Department, Reserve Bank of India and has been conceptualized by the office of Ombudsman, Mumbai-II.



Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks





1. Phishing links

Modus Operandi

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.



Precautions

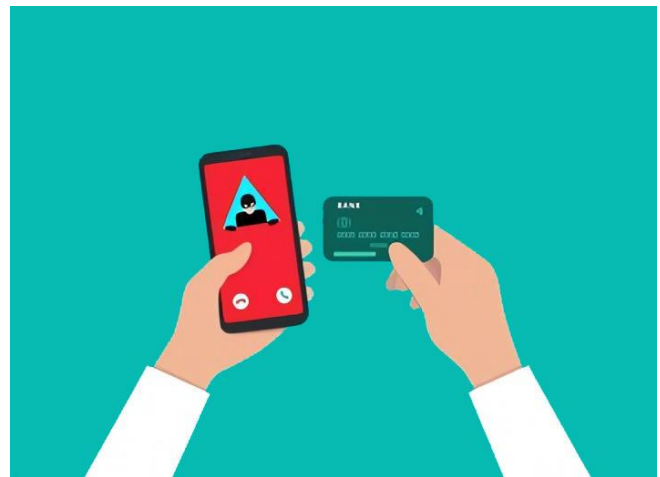
- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform



2. Vishing calls

Modus Operandi

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



Precautions

- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.



3. Frauds using online sales platforms

Modus Operandi

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is **no need to enter PIN / password** anywhere to **receive** money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.



4. Frauds due to the use of unknown / unverified mobile apps

Modus Operandi

- Fraudsters circulate through SMS / email / social media / Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before / after installation of such apps.



Precautions

- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.
- As a prudent practice before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.



5. ATM card skimming

Modus Operandi

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.



Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.



6. Frauds using screen sharing app / Remote access

Modus Operandi

- Fraudsters trick the customer to download a screen sharing app.
- Using such app, the fraudsters can watch / control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorised transfer of funds or make payments using the customer's Internet banking / payment apps.



Precautions

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.



7. SIM swap / SIM cloning

Modus Operandi

- Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.



Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.



8. Frauds by compromising credentials on results through search engines

Modus Operandi

- Customers use search engines to obtain contact details / customer care numbers of their bank, insurance company, Aadhaar updation centre, etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- Customers may end up contacting unknown / unverified contact numbers of the fraudsters displayed as bank / company's contact numbers on search engine.
- Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials / details for verification.
- Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.



Precautions

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- Please also note that customer care numbers are never in the form of mobile numbers.



9. Scam through QR code scan

Modus Operandi

- Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.
- By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.



Precautions

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.



10. Impersonation on social media

Modus Operandi

- Fraudsters create fake accounts using details of the users of social media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users' trust over a period of time. When the users share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.



Precautions

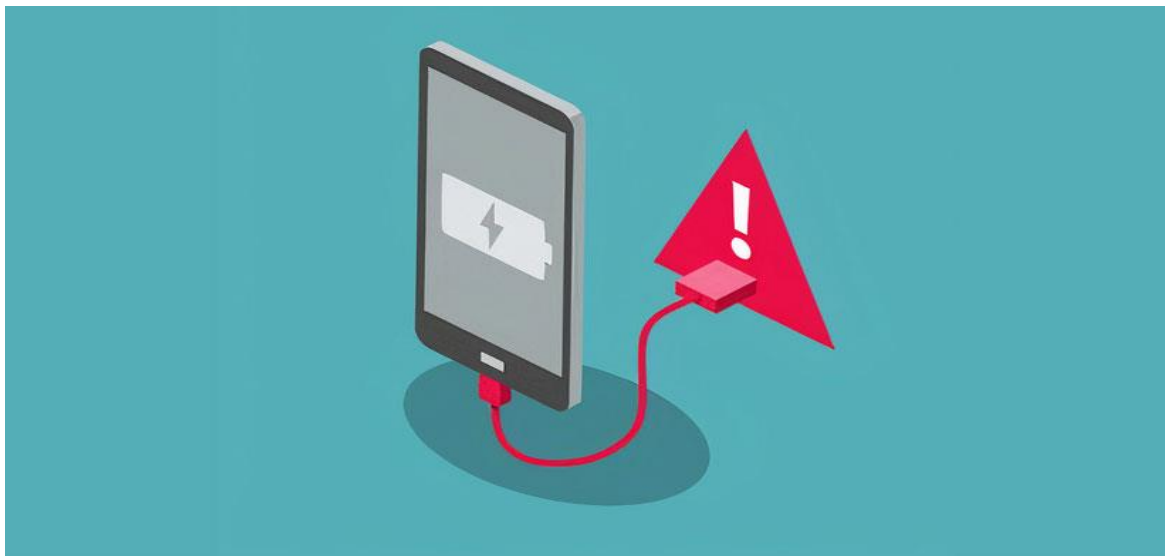
- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.



11. Juice jacking

Modus Operandi

- The charging port of a mobile, can also be used to transfer files / data.
- Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).



Precaution

- Avoid using public / unknown charging ports / cables.



12. Lottery fraud

Modus Operandi

- Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account / credit card details on a website from which data is captured by the fraudsters.
- Fraudsters also ask the customers to pay taxes/ forex charges / upfront or pay the shipping charges, processing / handling fee, etc., to receive the lottery / product.
- Fraudsters in some cases, may also pose as a representative of RBI or a foreign bank / company / international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.
- Since the requested money is generally a very small percentage of the promised lottery / prize, the customer may fall into the trap of the fraudster and make the payment.



Precautions

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.



13. Online job fraud

Modus Operandi

- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / credit card / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.



Precautions

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.



14. Money mules

Modus Operandi

- Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen / illegal money via their bank account/s.



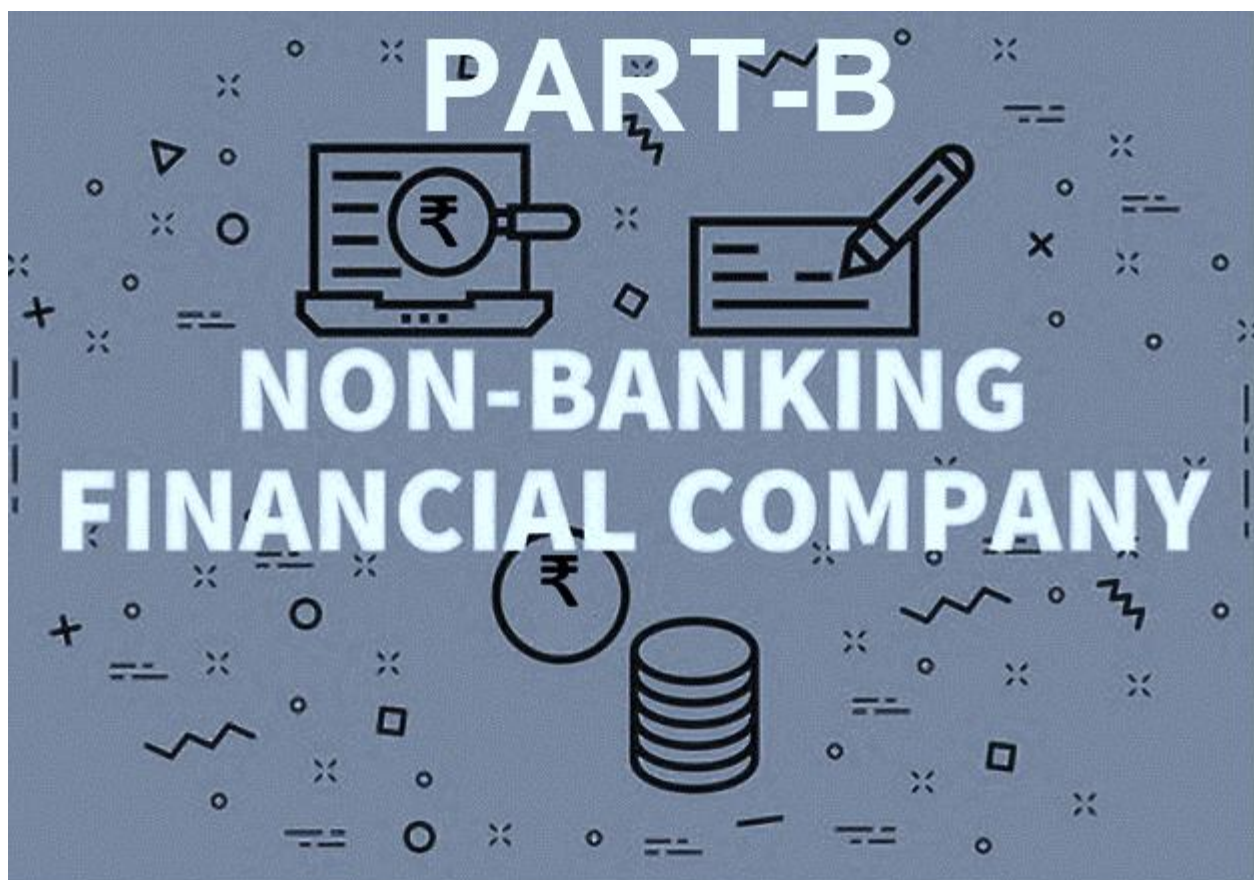
- Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions.
- The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Alternatively, the fraudster may direct the money mule to withdraw cash and hand it over to someone.
- When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

Precautions

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee.
- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.



Modus Operandi and Precautions to be taken against Fraudulent Transactions – Non Banking Financial Companies (NBFCs)





1. Fake advertisements for extending loans by fraudsters

Modus Operandi

- Fraudsters issue fake advertisements offering personal loans at very attractive and low rates of interest or easy repayment options or without any requirement of collateral/ security, etc.
- Fraudsters send emails with such offers and ask the borrowers to contact them. To gain credibility with the gullible borrowers and to induce confidence, these email-ids are made to look-like the emails IDs of senior officials of well-known / genuine Non-Banking Financial Companies (NBFCs).
- When borrowers approach the fraudsters for loans, the fraudsters take money from the borrowers in the name of various upfront charges like processing fees, Goods and Services Tax (GST), intercity charge, advance Equated Monthly Instalment (EMI), etc., and abscond without disbursing the loans.
- Fraudsters also create fake website links to show up on search engines, when people search for information on loans.



Precautions

- Loan processing fee charged by NBFCs / banks is deducted from the sanctioned loan amount and not demanded upfront in cash from the borrower.
- Never pay any processing fee in advance as NBFCs / banks will never ask for an advance fee before the processing of loan application.
- Do not make payments or enter secure credentials against online offer of loans at low interest rates, etc., without checking / verifying the particulars through genuine sources.



2. SMS / Email / Instant Messaging / Call scams

Modus Operandi

- Fraudsters circulate fake messages in instant messaging apps / SMS / social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.
- The fraudsters may even share their Aadhaar card / Pan Card and fake NBFC ID card.
- After sending such bulk messages / SMS / emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.



Precautions

- Never believe loan offers made by people on their own through telephones / emails, etc.
- Never make any payment against such offers or share any personal / financial credentials against such offers without cross-checking that it is genuine through other sources.
- Never click on links sent through SMS / emails or reply to promotional SMS / emails.
- Never open / respond to emails from unknown sources containing suspicious attachment or phishing links.



3. OTP based Frauds

Modus Operandi

- Fraudsters impersonating as NBFCs, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number.
- When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.



Precautions

- Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.
- Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.
- Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications.

Modus Operandi

-
- This collection of 12 isometric illustrations depicts a purple-robed hacker character engaged in various cyber activities. The hacker is shown interacting with a laptop, a smartphone, a tablet, and a desktop computer. The devices display various symbols: a padlock, a skull and crossbones, a shield, and a network diagram. The hacker is also shown holding a yellow shield, a yellow bag, and a yellow cube, which may represent different types of data or threats. The illustrations are arranged in a grid-like pattern, with the hacker character appearing in multiple instances, each performing a different action.

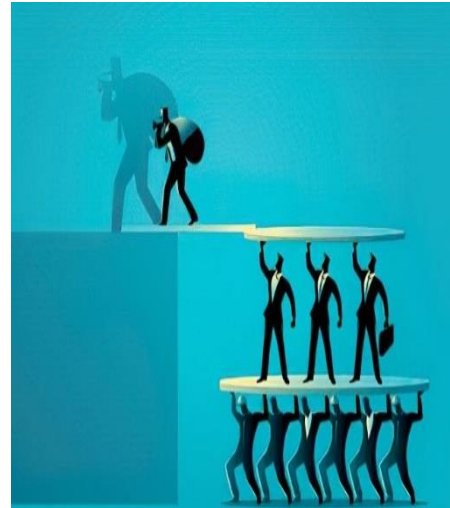
- Verify if the lender is registered with the Government / Regulator /authorised agencies
- Check whether the lender has provided a physical address or contact information to ensure it is not difficult to contact them later.
- Beware if the lender appears more interested in obtaining personal details rather than in checking credit scores.
- Remember that any reputed NBFC / bank will never ask for payment before processing the loan application.
- Genuine loan providers never offer money without verifying documents and other credentials of the borrowers.
- Verify if these NBFC-backed loan apps are genuine.



5. Money circulation / Ponzi / Multi-Level Marketing (MLM) schemes fraud

Modus Operandi

- Fraudsters use MLM / Chain Marketing / Pyramid Structure schemes to promise easy or quick money upon enrolment / adding of members.
- The schemes not only assure high returns but also pay the first few instalments (EMIs) to gain confidence of gullible persons and attract more investors through word of mouth publicity.
- The schemes encourage addition of more people to the chain / group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.
- This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.



Precautions

- Returns are proportional to risks. Higher the return, higher is the risk.
- Any scheme offering abnormally high returns (40-50% p a) consistently, could be the first sign of a potential fraud and caution needs to be exercised.
- Always notice that any payment / commission / bonus / percentage of profit without the actual sale of goods / service is suspicious and may lead to a fraud.
- Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing / Chain Marketing / Pyramid Structure schemes.
- Acceptance of money under Money Circulation / Multi-level Marketing / Pyramid structures is a cognizable offence under the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- In case of such offers or information of such schemes, a complaint must be immediately lodged with the State Police.



6. Fraudulent loans with forged documents

Modus Operandi

- Fraudsters use forged documents to avail services from financial institutions.
- Fraudsters commit identity thefts, steal personal information of customers such as identity cards, bank account details etc., and use this information or credentials to avail benefits from a financial institution.
- Fraudsters pose as NBFC employees and collect KYC related documents from customers.



Precautions

- Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.
- Such documents should be shared only with the entity's authorised personnel or on authorised email IDs of the entities.
- Follow up with the concerned entities to ensure that the documents shared by you are purged immediately by them in case of non-sanction of loan and/ or post closure of the loan account.



General Precautions to be taken for financial transactions





General precautions

- Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (<https://> - URL with a pad lock symbol) before making online payments / transactions.
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites / devices / public laptop / desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.



For device / computer security

- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Always scan unknown Universal Serial Bus (USB) drives / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices.





For safe internet browsing

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.

For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.





Factors indicating that a phone is being spied

- Unfamiliar applications are being downloaded on the phone.
- There is a faster than usual draining of phone battery.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.
- An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background.
- Spyware apps might sometimes interfere with a phone's shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.
- Note that text messages can be used by spyware and malware to send and receive data.

Actions to be taken after occurrence of a fraud

- Block not only the debit card / credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the **official customer care number** available on the bank's website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.
- Dial helpline number 155260 or 1930 or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in).
Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile.

Precautions related to Debit / Credit cards

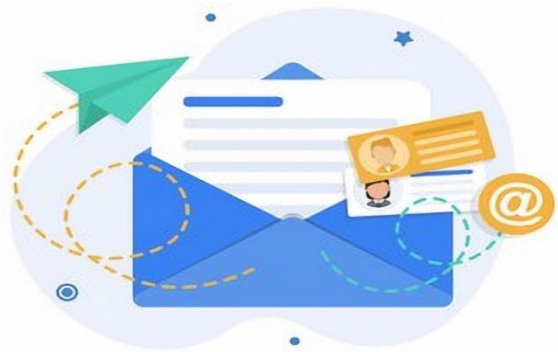
- You should deactivate various features of credit / debit card, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.



- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Cover the keypad with your other hand while entering the PIN at a POS site / ATM.

For E-mail account security

- Do not click on links sent through emails from unknown addresses / names.
- Avoid opening emails on public or free networks.
- Do not store secure credentials / bank passwords, etc., in emails.



For password security

- Use a combination of alphanumeric and special characters in your password.
- Keep two factor authentication for all your accounts, if such facility is available.
- Change your passwords periodically.
- Avoid having your date of birth, spouse name, car number etc. as passwords.





How do you know whether an NBFC accepting deposit is genuine or not?

- Verify whether the name of NBFC appears in the list of deposit taking NBFCs entitled to accept deposits, available at <https://rbi.org.in> and to ensure that it is not appearing in the list of companies prohibited from accepting deposits.
- NBFCs must prominently display the Certificate of Registration (CoR) issued by the Reserve Bank on its site / in its office. This certificate should also reflect that the NBFC has been specifically authorised by RBI to accept deposits. Scrutinize the certificate to ensure that the NBFC is authorised to accept deposits.
- NBFCs cannot accept deposits for a period less than 12-months and more than 60 months and the maximum interest rate that an NBFC can pay to a depositor should not exceed 12.5%.
- The Reserve Bank publishes the change in the interest rates on <https://rbi.org.in> → Sitemap → NBFC List → FAQs.





Precautions to be taken by depositors

- When depositing money, insist on a proper receipt for each and every deposit made with the bank / NBFC / company.
- The receipt should be duly signed by an officer authorised by the company and should state, *inter alia*, the date of the deposit, the name of the depositor, the amount in words and figures, rate of interest payable, maturity date and amount.
- In the case of brokers / agents, etc., collecting public deposits on behalf of NBFCs, verify that the brokers / agents are duly authorised for the purpose by the concerned NBFC.
- Remember that the Deposit Insurance facility is not available to depositors of NBFCs.





File a complaint

Complaint to RBI Ombudsman

- For filing complaints online, please visit the link at <https://cms.rbi.org.in/>
- Complaints in physical / paper form can be sent to CRPC, Reserve Bank of India, Central Vista, Sector -17, Chandigarh -160 017.

Complaint to Securities and Exchange Board of India (SEBI)

- Please visit the link at <https://www.sebi.gov.in/>

Complaint to Insurance Regulatory and Development Authority of India (IRDAI)

- Please visit the link at <https://www.irdai.gov.in/>

Complaint to National Housing Bank (NHB)

- Please visit the link at <https://nhb.org.in/>

Complaint to Cyber Police Station

- Please visit <https://cybercrime.gov.in/>



Glossary

- **Advance fee/Processing fee/Token fee:** These include preliminary payments such as documentation charges, meeting expenses, processing fees, other charges that may be applicable for disbursement of the loan to a borrower.
- **Two-factor authentication:** Authentication methodologies involve three basic 'factors'- something the user knows (e.g., password, PIN- either static or one time generated); something the user has (e.g., ATM/ smart card number, expiry date and CVV that is printed on the card); and something the user is (e.g., biometric characteristic, such as a fingerprint). Two-factor authentication (also known as 2FA) provides identification of users by means of a combination of two different components - what the user has and what the user knows/is to complete a transaction.
- **Authorisation:** The response from a card-issuing bank to a merchant's transaction authorisation request indicating that the payment information is valid and funds are available on the customer's credit card.
- **Card number:** The number assigned by a credit card association or card issuing bank to a card. This information must be provided to a merchant by a customer in order to make a credit card payment but should not be shared with anyone else. The string of digits is printed on the card.
- **Credit card:** A card that allows paying for products or services by availing unsecured/secured credit from a financial institution.
- **Credit limit:** The term refers to the maximum amount of credit a financial institution extends to a customer. A lending institution extends a credit limit on a credit card based on the analysis of the information given by the credit-seeking applicant. The credit limit can affect the customer's credit scores and their ability to obtain credit in the future.
- **CVV:** Stands for Card Verification Value. This is a 3-digit number printed on the card which is mandatory for completing most online transactions. These details are confidential and must NEVER be shared with anyone.
- **Debit card:** A card that allows paying for products or services by deduction of available funds in a bank account of the cardholder.



- **E-commerce platform:** It is a platform/website that enables buying and selling of goods and services including digital products over digital and electronic network.
- **EMI:** It stands for Equated Monthly Instalment. This a fixed monthly payment (includes principal and interest) to be made by a borrower to his lender/creditor (like bank/NBFC) each month till the loan/credit, along with interest, taken from the lender/creditor is paid off by the borrower in full.
- **Encryption:** The process of transforming processing information into an electronic code to maintain its secrecy.
- **Expiry date:** The date on which the validity of a card, contract, agreement, document, etc. expires. Transactions will be approved only in respect of cards or documents which have not yet expired.
- **Gateway:** It is an intermediary that provides technology infrastructure to route and facilitate processing of services such as transactions base management, risk management, etc. without its involvement directly. Payment Gateways are entities that provide technology infrastructure to route and facilitate processing of online payment transactions without any involvement in handling of funds.
- **Immediate payment services (IMPS):** It is an instant interbank electronic fund transfer service (up to a limit) through mobile phones, provided by National Payments Corporation of India (NPCI).
- **KYC:** Stands for Know Your Customer. It is process in which the financial institution makes an effort to verify the identity, suitability, and risks involved with maintaining a relationship with a customer by obtaining a set of documents and carrying out due diligence.
- **Money mule:** It is a term used to describe victims who are exploited by fraudsters into laundering stolen / illegal money via their bank account(s).
- **Multi-Level Marketing:** The practice of selling goods or services on behalf of a company in a system whereby participants receive commission on their sales as well as the sales of any participants they recruit.



- **National Automated Clearing House (NACH):** It is a centralised Electronic Clearing Service (ECS) system operated by National Payments Corporation of India (NPCI).
- **Near Field Communication (NFC):** It is a communication technology used to transmit data from a NFC equipped device to a capable terminal. The NFC technology is used to make a contactless payment that is carried out by keeping the smartphone/card near the NFC enabled machine.
- **National Electronic Fund Transfer (NEFT):** It is a nation-wide centralised payment system owned and operated by RBI, which enables bank customers in India to transfer funds between any two NEFT-enabled bank accounts.
- **OTP:** One Time Password is one of the factors in the authentication methodology, which the customer knows and is often used for carrying out online transactions. This is CONFIDENTIAL and should not be shared with anyone.
- **Phishing:** It refers to spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.
- **Point of Sale device (POS) / Acceptance Device (mPOS):** It refers to any device / terminal / machine installed at Merchant Establishments which enables the merchants to accept payments through payment cards (credit cards, debit cards, gift cards etc.).
- **Quick Response (QR) code:** The QR Code is type of a two-dimensional bar code. It consists of black squares arranged in a square grid on a white background. Imaging devices such as smartphone cameras can be used to read and interpret these codes. QR code contains information about the payee and is used to facilitate mobile payments at the point-of-sale by debiting the customers' account.
- **Remote Access:** It refers to luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.



- **UPI:** Unified Payment Interface is a platform that allows transfer of money from one bank / wallet account to other using a mobile phone which has access to the Internet. Once a customer registers for UPI with the bank, a unique virtual identifier is created and mapped to the customer's mobile phone to initiate the payment. It uses authentication in the form of UPI-PIN, which is CONFIDENTIAL and should not be shared with anyone.
- **Vishing:** It refers to phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers luring customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.
- **Wallet:** A wallet is like an account which can be used for purchase of goods and services against the stored value in it. A wallet can be virtual (e.g. mobile wallet) or physical (prepaid cards).



(10)

Government of Arunachal Pradesh
Finance, Planning & Investment Department
Economic Affairs Division :: A.P. Civil Secretariat : Itanagar

No. 16-22018/1/2022-EA BRANCH

Dated Itanagar the 21st April, 2023

To

1. The DIGP,
Government of Arunachal Pradesh
Itanagar
2. The Secretary Information Technology(IT)
Government of Arunachal Pradesh
Itanagar

Sub:- Minutes of the Round 12 Meeting of State Level Coordination Committee (SLCC) for the State of Arunachal Pradesh – Initiations of actions on the action points emanated during the SLCC Meeting also submit action taken report thereof.

Sir,

I am directed to enclose herewith copy of the Minutes of the Round 12 Meeting of State Level Coordination Committee (SLCC) for the State of Arunachal Pradesh held on 20th January 2023 under the Chairmanship of the Principal Secretary Finance, Govt. of Arunachal Pradesh, Itanagar and to request you to take actions on the action points emanated from the meeting and submit Action Taken Report to this office at an earliest possible.

Enclosed : As above

Yours Sincerely,

Amc
21/04/2023

(Tapi Loma),
Under Secretary, Finance (EA)
Govt. of Arunachal Pradesh
Itanagar

Memo No. 16-22018/1/2022-EA BRANCH

Dated Itanagar the 21st April, 2023

Copy To:

1. The Under Secretary to Chief Secretary, Govt. of Arunachal Pradesh for information please.
2. P.S to Principal Secretary Finance, Govt. of Arunachal Pradesh, Itanagar.
3. SPA to Secretary Finance, Govt. of Arunachal Pradesh, Itanagar.
4. Office Copy.

1 AMC
21/4/23



Reserve Bank of India

Guwahati

Minutes of Round 12 Meeting of the State Level Co-ordination Committee (SLCC) for the State of Arunachal Pradesh on Regulation of Non-Banking Financial Companies (NBFCs) and Un-Incorporated Bodies (UIBs) held on January 20, 2023

Round 12 Meeting of the SLCC for the State of Arunachal Pradesh on Regulation of NBFCs and UIBs was held on January 20, 2023 at 11:00 AM at Chief Secretary Conference Hall, Itanagar, Arunachal Pradesh. The meeting was chaired by Dr. Sharat Chauhan, IAS, Principal Secretary (Finance), Government of Arunachal Pradesh and convened by Shri Haridas Sarode, Deputy General Manager, Reserve Bank of India (RBI), Guwahati. Senior officials of the Finance Department, Home Department, Police Department of Arunachal Pradesh; RBI, Securities Exchange Board of India (SEBI) and Member of ICAI participated in the meeting. The list of the participants is furnished in the Annex.

2. The Deputy General Manager (DGM), RBI, in his welcome address, extended warm welcome to the Chairman and all the members of the SLCC for the State of Arunachal Pradesh. Highlighting the importance of the forum, he stated that the forum facilitates cooperation and co-ordination amongst the financial sector regulators and law enforcement authorities for taking timely & effective action against the entities engaged in unauthorized collection of funds/ deposits from public with fraudulent intentions. The DGM also apprised the forum that functioning of the SLCC is periodically reviewed by the Sub Committee of the Financial Stability and Development Council (FSDC-SC).

Dr. Sharat Chauhan, IAS, Principal Secretary (Finance), Government of Arunachal Pradesh and the Chairman, SLCC, in his opening remarks highlighted the importance of conducting SLCC meetings and thereby acknowledged that such meetings should be held at regular intervals for creation of financial awareness among all stakeholders.

3. Confirmation of the minutes of the previous meeting:

There was no proposal for amendment to the minutes of the previous meeting and the same was confirmed without any modification.

4. Action taken in respect of items discussed during the previous meeting:

(i) Timely conduct of SLCC Meetings:

Regrading timely conduct of SLCC Meeting for the State of Arunachal Pradesh, the Chairman proposed the next Round of SLCC Meeting may be scheduled during last week of April 2023. He further suggested that the possibility of conducting such meetings in online or hybrid mode can also be explored in this regard. Considering this, Finance Department, Government of Arunachal Pradesh may confirm the date and mode of the next Round of SLCC Meeting for the State.

[Action: Finance Department, Govt. of Arunachal Pradesh]

(ii) Arrangement of integrated training programme for trainers at Police Training Centre (PTC):

The Chairman observed that the Police Department is required to take suitable initiatives for conducting integrated training programme for the Police Officials of the State and as such he advised to re initiate the entire action point from the previous meeting.

[Action: Police Department, Govt. of Arunachal Pradesh]

Principal Secretary (Home), Government of Arunachal Pradesh observed that trainings imparted at PTC, Banderdawa is normally for the constabulary and therefore he advised that Police Department, Government of Arunachal Pradesh may take up the matter with NEPA, Shillong and make suitable request to RBI for required faculty support.

[Action: Police Department, Govt. of Arunachal Pradesh and RBI]

The Chairman further suggested that alternatively, Finance Department, Government of Arunachal Pradesh can organize a one-day (of approx. three hours duration) awareness programme at the Secretariat for the senior officials of the Government of Arunachal Pradesh followed by another such programme for police officials of the state on the next day at the same venue. Finance Department, Government of Arunachal Pradesh may request RBI & SEBI for necessary faculty support in this regard.

[Action: Finance Department, Govt. of Arunachal Pradesh]

(iii) Review of conduct of Awareness Programmes carried out by regulators since the last meeting:

In order to encourage electronic payment systems for ushering in a less-cash society in India and to ensure a safe, secure, efficient, interoperable, convenient payment systems and creating financial awareness among Government officials and members of public, RBI has been organizing awareness programmes across the country. Relevant material in connection with digital awareness of the members of the public was shared by RBI with the Finance Department of the State. RBI also shared hard copy of the booklet 'BE(A)WARE-A booklet on Modus Operandi of Financial Fraudsters' on the day of the meeting. The Chairman advised the Secretary, Finance Department to share the material with the IT Department of the State to enable the department to put the material on the Government website for greater interest of the public.

[Action: Finance Department, Govt. of Arunachal Pradesh]

DGM, SEBI apprised the forum that they had conducted a training programme for the Police Officials for the State of Mizoram.

DGM, SEBI highlighted that there is only one resource person in the state of Arunachal Pradesh and as such they had invited application for enrolment as resource person. The Chairman advised the Secretary, Finance Department, Government of Arunachal Pradesh and SEBI to write to the Rajiv Gandhi University to encourage commerce and economics background students to apply for empanelment as resource persons.

[Action: Finance Department, Govt. of Arunachal Pradesh; SEBI]

(iv) The Banning of Unregulated Deposit Scheme Act, 2019:

The Secretary, Finance Department apprised the forum that the draft rules under the BUDS Act, 2019 have been framed by the State Government along with appointment of Competent Authority. The draft rules have been forwarded to Ministry of Finance, Government of India for vetting / approval. The Chairman advised the Secretary, Finance Department to follow up with DFS, Ministry of Finance, Government of India to expedite the implementation of BUDS Act, 2019 in the state.

[Action: Finance Department, Govt. of Arunachal Pradesh]

5. Updates on implementation of BUDS Act, 2019 in the State of Arunachal Pradesh

The matter has been highlighted in Para 4(iv) above.

6. Sharing of information relating to acceptance of public deposits etc. by various entities:

The forum was apprised of the unauthorized acceptance of public deposits /lending activities by various unauthorized entities viz., LFS Broking, Euro Exim Bank, RDQ Stock Broking etc. DGM, RBI requested the forum on sharing of information on similar cases from the State of Arunachal Pradesh. To this, the Chairman advised the SP (Crime), Government of Arunachal Pradesh to share unique financial fraud cases across the State with RBI which can be shared by RBI on other SLCC or SLCC-Sub Committee forums of other states and benefit members of these forums to get early leads, if any.

The Chairman appreciated the presentations given by RBI at the forum and acknowledged its usefulness to the members in gaining additional knowledge.

[Action: Police Department, Govt. of Arunachal Pradesh]

7. Review of conduct of Awareness Programmes carried out by various regulators since the last meeting:

The matter has been highlighted in Para 4 (iii) above.

8. With the permission of the Chairman, DGM, RBI initiated the discussion in connection to poor financial health of the Arunachal Pradesh State Co-operative Bank. The Chairman advised Registrar of Cooperative Society (RCS), Government of Arunachal Pradesh to explore a solution in consultation with all the stakeholders. The discussion remained inconclusive since no officials from the RCS, Government of Arunachal Pradesh was present at the meeting.

[Action: RCS, Govt. of Arunachal Pradesh]

9. The meeting concluded with a vote of thanks to the Chair and other members.

Annex

List of Participants

Sl. No.	Name	Designation and Department / Organization
(i) Government of Arunachal Pradesh		
1	Dr. Sharat Chauhan, IAS	Principal Secretary, Finance (Chairman)
2	Shri Kaling Tayeng, IAS	Principal Secretary, Home
3	Smt. Y W Ringu, IAS	Secretary (Finance)
4	Shri Michi Paku, IPS	IGP, Security/ Training
5	Shri Takhe Kani	Deputy Secretary, Finance
(ii) Reserve Bank of India		
1	Shri Haridas Bapurao Sarode	Deputy General Manager, Guwahati
2	Shri Niraj Kumar	Assistant General Manager, Guwahati
3	Shri Kiran Paul	Manager, Guwahati
(iii) Other Regulators		
1	Shri Jangchon Lhouvum	Deputy General Manager, SEBI
2	CA Shweta Agarwala	Representative from ICAI

20

**Government of Arunachal Pradesh
Finance, Planning & Investment Department
(Economic Affairs Branch)
Itanagar.**

No. FIN/EA-25/2011(Vol-II)

Dated Itanagar, the 1st May, 2023.

To,

**The Secretary,
Department of Information Technology,
Arunachal Pradesh,
Itanagar.**

Subject:- Awareness Programme on Financial Literacy – Regarding.

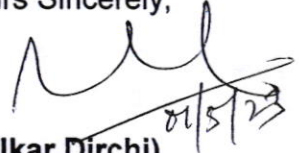
Sir,

With reference to the subject cited above, I am directed to forward herewith a hard copy of a booklet 'BE(A)WARE - A booklet on Modus Operandi of Financial Fraudsters' shared by the Reserve Bank of India with a request to put up the material (booklet) on the Government Website for greater interest of the public.

This is for favour of your information and necessary action please.

Enclosed: As stated above.

Yours Sincerely,



**(Ikar Dirchi)
Joint Secretary (Finance)
Govt. of Arunachal Pradesh,
Itanagar.**

Dated Itanagar, the 1st May, 2023.

Memo No. FIN/EA-25/2011(Vol-II) *375*
Copy for information to:-

1. The US to the Chief Secretary, Govt. of Arunachal Pradesh, Itanagar.
2. The PS to Principal Secretary(Finance), Govt. of Arunachal Pradesh, Itanagar.
3. The SPA to Secretary(Finance), Govt. of Arunachal Pradesh, Itanagar.
- ✓ 4. Office copy.



**(Ikar Dirchi)
Joint Secretary (Finance)
Govt. of Arunachal Pradesh,
Itanagar.**

*1852
21/5/23*

BE(A)WARE



**A BOOKLET
ON
MODUS OPERANDI
OF
FINANCIAL FRAUDSTERS**



RESERVE BANK OF INDIA





Table of Contents

	Subject	Page No.
	<u>Preface</u>	1
	<u>Part A - Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks</u>	2
1	<u>Phishing links</u>	3
2	<u>Vishing calls</u>	4
3	<u>Frauds using online sales platforms</u>	5
4	<u>Frauds due to the use of unknown / unverified mobile apps</u>	6
5	<u>ATM card skimming</u>	7
6	<u>Frauds using screen sharing app / Remote access</u>	8
7	<u>SIM swap / SIM cloning</u>	9
8	<u>Frauds by compromising credentials through search engines</u>	10
9	<u>Scam through QR code scan</u>	11
10	<u>Impersonation on social media</u>	12
11	<u>Juice jacking</u>	13
12	<u>Lottery frauds</u>	14
13	<u>Online job frauds</u>	15
14	<u>Money mules</u>	16
	<u>Part B - Modus Operandi and Precautions to be taken against Fraudulent Transactions - NBFCs</u>	17
1	<u>Fake advertisements for grant of loans</u>	18
2	<u>SMS / Email / Instant Messaging / Call scam</u>	19
3	<u>OTP based frauds</u>	20
4	<u>Fake loan websites / App frauds</u>	21
5	<u>Money circulation / Ponzi / Multi-Level Marketing (MLM) scheme frauds</u>	22
6	<u>Loans with forged documents</u>	23
	<u>Part C - General precautions to be taken for financial transactions</u>	24
	<u>Glossary</u>	32



Preface

There has been a surge in usage of digital modes of payment in the recent years. This gained further momentum during the Covid-19 induced lockdowns. While enhancing customer convenience, it also furthered the national objective of financial inclusion. However, as the speed and ease of doing financial transactions has improved, the number of frauds reported in retail financial transactions have also gone up. Fraudsters have been using innovative methods to defraud the common and gullible people of their hard-earned money, especially the new entrants in the use of digital platforms who are not entirely familiar with the techno-financial eco-system.

This booklet has been compiled from various incidents of frauds reported as also from complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are inexperienced, or not so experienced, in digital and electronic modes of financial transactions. The booklet is intended to create awareness among the members of public about the modus operandi adopted by fraudsters to defraud and mislead them, while also informing them about the precautions to be taken while carrying out financial transactions. It emphasizes the need for keeping one's personal information, particularly the financial information, confidential at all times, be-ware of unknown calls / emails / messages, practicing due diligence while performing financial transactions and changing the secure credentials / passwords from time to time. Hence the title **BE(A)WARE** – Be Aware and Beware!

This booklet is part of the public awareness initiative by the Consumer Education and Protection Department, Reserve Bank of India and has been conceptualized by the office of Ombudsman, Mumbai-II.



Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks





1. Phishing links

Modus Operandi

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.



Precautions

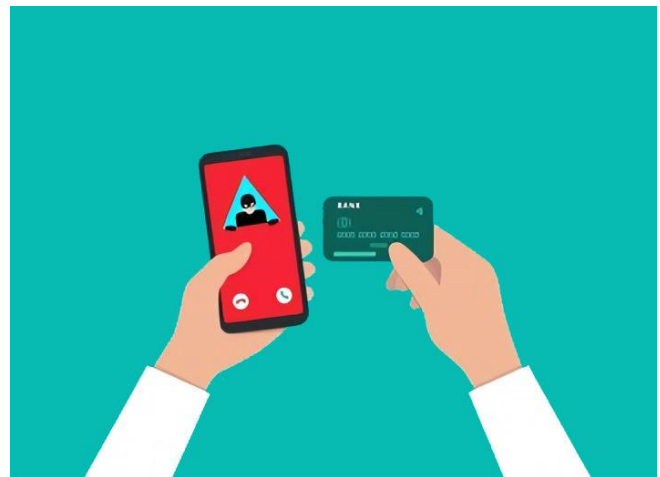
- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform



2. Vishing calls

Modus Operandi

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



Precautions

- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.



3. Frauds using online sales platforms

Modus Operandi

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is **no need to enter PIN / password** anywhere to **receive** money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.



4. Frauds due to the use of unknown / unverified mobile apps

Modus Operandi

- Fraudsters circulate through SMS / email / social media / Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before / after installation of such apps.



Precautions

- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.
- As a prudent practice before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.



5. ATM card skimming

Modus Operandi

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.



Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.



6. Frauds using screen sharing app / Remote access

Modus Operandi

- Fraudsters trick the customer to download a screen sharing app.
- Using such app, the fraudsters can watch / control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorised transfer of funds or make payments using the customer's Internet banking / payment apps.



Precautions

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.



7. SIM swap / SIM cloning

Modus Operandi

- Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.



Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.



8. Frauds by compromising credentials on results through search engines

Modus Operandi

- Customers use search engines to obtain contact details / customer care numbers of their bank, insurance company, Aadhaar updation centre, etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- Customers may end up contacting unknown / unverified contact numbers of the fraudsters displayed as bank / company's contact numbers on search engine.
- Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials / details for verification.
- Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.



Precautions

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- Please also note that customer care numbers are never in the form of mobile numbers.



9. Scam through QR code scan

Modus Operandi

- Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.
- By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.



Precautions

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.



10. Impersonation on social media

Modus Operandi

- Fraudsters create fake accounts using details of the users of social media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users' trust over a period of time. When the users share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.



Precautions

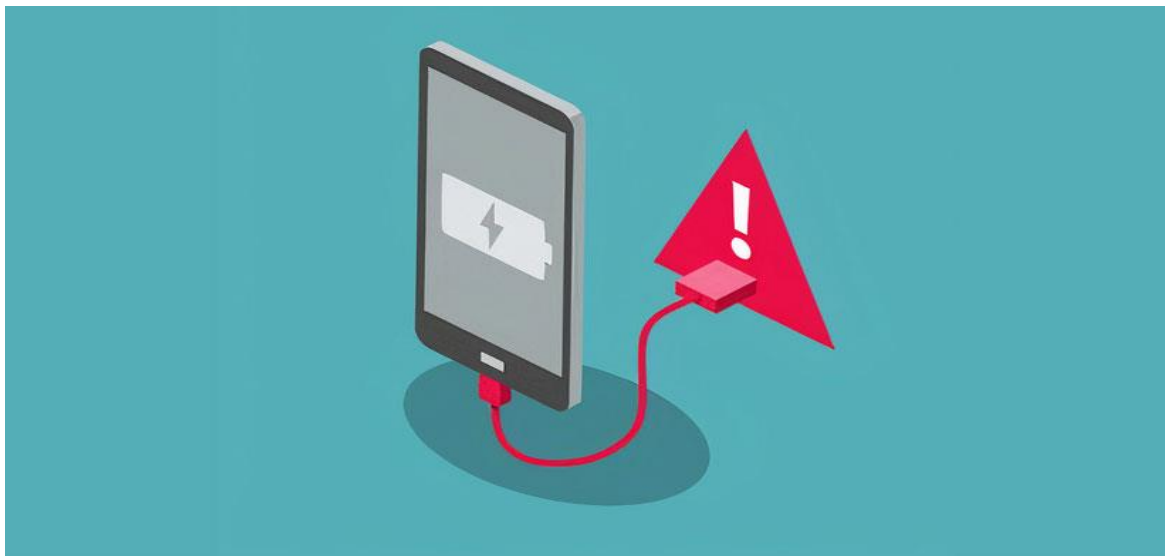
- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.



11. Juice jacking

Modus Operandi

- The charging port of a mobile, can also be used to transfer files / data.
- Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).



Precaution

- Avoid using public / unknown charging ports / cables.



12. Lottery fraud

Modus Operandi

- Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account / credit card details on a website from which data is captured by the fraudsters.
- Fraudsters also ask the customers to pay taxes/ forex charges / upfront or pay the shipping charges, processing / handling fee, etc., to receive the lottery / product.
- Fraudsters in some cases, may also pose as a representative of RBI or a foreign bank / company / international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.
- Since the requested money is generally a very small percentage of the promised lottery / prize, the customer may fall into the trap of the fraudster and make the payment.



Precautions

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.



13. Online job fraud

Modus Operandi

- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / credit card / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.



Precautions

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.



14. Money mules

Modus Operandi

- Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen / illegal money via their bank account/s.



- Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions.
- The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Alternatively, the fraudster may direct the money mule to withdraw cash and hand it over to someone.
- When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

Precautions

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee.
- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.



Modus Operandi and Precautions to be taken against Fraudulent Transactions – Non Banking Financial Companies (NBFCs)





1. Fake advertisements for extending loans by fraudsters

Modus Operandi

- Fraudsters issue fake advertisements offering personal loans at very attractive and low rates of interest or easy repayment options or without any requirement of collateral/ security, etc.
- Fraudsters send emails with such offers and ask the borrowers to contact them. To gain credibility with the gullible borrowers and to induce confidence, these email-ids are made to look-like the emails IDs of senior officials of well-known / genuine Non-Banking Financial Companies (NBFCs).
- When borrowers approach the fraudsters for loans, the fraudsters take money from the borrowers in the name of various upfront charges like processing fees, Goods and Services Tax (GST), intercity charge, advance Equated Monthly Instalment (EMI), etc., and abscond without disbursing the loans.
- Fraudsters also create fake website links to show up on search engines, when people search for information on loans.



Precautions

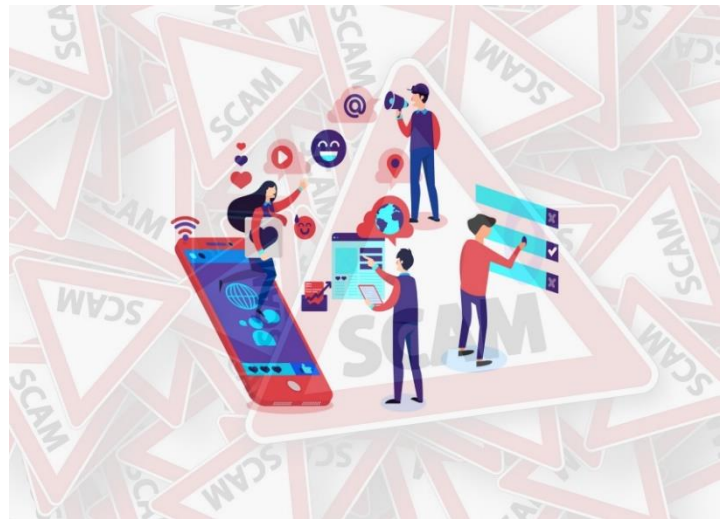
- Loan processing fee charged by NBFCs / banks is deducted from the sanctioned loan amount and not demanded upfront in cash from the borrower.
- Never pay any processing fee in advance as NBFCs / banks will never ask for an advance fee before the processing of loan application.
- Do not make payments or enter secure credentials against online offer of loans at low interest rates, etc., without checking / verifying the particulars through genuine sources.



2. SMS / Email / Instant Messaging / Call scams

Modus Operandi

- Fraudsters circulate fake messages in instant messaging apps / SMS / social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.
- The fraudsters may even share their Aadhaar card / Pan Card and fake NBFC ID card.
- After sending such bulk messages / SMS / emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.



Precautions

- Never believe loan offers made by people on their own through telephones / emails, etc.
- Never make any payment against such offers or share any personal / financial credentials against such offers without cross-checking that it is genuine through other sources.
- Never click on links sent through SMS / emails or reply to promotional SMS / emails.
- Never open / respond to emails from unknown sources containing suspicious attachment or phishing links.



3. OTP based Frauds

Modus Operandi

- Fraudsters impersonating as NBFCs, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number.
- When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.



Precautions

- Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.
- Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.
- Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications.

Modus Operandi

-
- This collection of 12 isometric illustrations depicts a purple-robed hacker character engaged in various cyber activities. The hacker is shown interacting with a laptop, a smartphone, a tablet, and a desktop computer. The devices display various symbols: a padlock, a skull and crossbones, a shield, a magnifying glass, a document, and a network diagram. The hacker is also shown holding a yellow shield, a yellow bag, and a yellow cube, which may represent different types of data or threats. The illustrations are arranged in a grid-like pattern, with the hacker character appearing in multiple instances, each performing a different action.

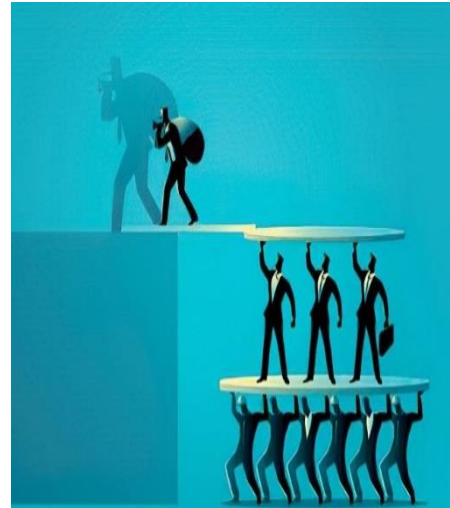
- Verify if the lender is registered with the Government / Regulator /authorised agencies
- Check whether the lender has provided a physical address or contact information to ensure it is not difficult to contact them later.
- Beware if the lender appears more interested in obtaining personal details rather than in checking credit scores.
- Remember that any reputed NBFC / bank will never ask for payment before processing the loan application.
- Genuine loan providers never offer money without verifying documents and other credentials of the borrowers.
- Verify if these NBFC-backed loan apps are genuine.



5. Money circulation / Ponzi / Multi-Level Marketing (MLM) schemes fraud

Modus Operandi

- Fraudsters use MLM / Chain Marketing / Pyramid Structure schemes to promise easy or quick money upon enrolment / adding of members.
- The schemes not only assure high returns but also pay the first few instalments (EMIs) to gain confidence of gullible persons and attract more investors through word of mouth publicity.
- The schemes encourage addition of more people to the chain / group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.
- This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.



Precautions

- Returns are proportional to risks. Higher the return, higher is the risk.
- Any scheme offering abnormally high returns (40-50% p a) consistently, could be the first sign of a potential fraud and caution needs to be exercised.
- Always notice that any payment / commission / bonus / percentage of profit without the actual sale of goods / service is suspicious and may lead to a fraud.
- Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing / Chain Marketing / Pyramid Structure schemes.
- Acceptance of money under Money Circulation / Multi-level Marketing / Pyramid structures is a cognizable offence under the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- In case of such offers or information of such schemes, a complaint must be immediately lodged with the State Police.



6. Fraudulent loans with forged documents

Modus Operandi

- Fraudsters use forged documents to avail services from financial institutions.
- Fraudsters commit identity thefts, steal personal information of customers such as identity cards, bank account details etc., and use this information or credentials to avail benefits from a financial institution.
- Fraudsters pose as NBFC employees and collect KYC related documents from customers.



Precautions

- Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.
- Such documents should be shared only with the entity's authorised personnel or on authorised email IDs of the entities.
- Follow up with the concerned entities to ensure that the documents shared by you are purged immediately by them in case of non-sanction of loan and/ or post closure of the loan account.



General Precautions to be taken for financial transactions





General precautions

- Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (<https://> - URL with a pad lock symbol) before making online payments / transactions.
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites / devices / public laptop / desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.



For device / computer security

- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Always scan unknown Universal Serial Bus (USB) drives / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices.





For safe internet browsing

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.

For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.





Factors indicating that a phone is being spied

- Unfamiliar applications are being downloaded on the phone.
- There is a faster than usual draining of phone battery.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.
- An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background.
- Spyware apps might sometimes interfere with a phone's shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.
- Note that text messages can be used by spyware and malware to send and receive data.

Actions to be taken after occurrence of a fraud

- Block not only the debit card / credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the **official customer care number** available on the bank's website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.
- Dial helpline number 155260 or 1930 or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in).
Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile.

Precautions related to Debit / Credit cards

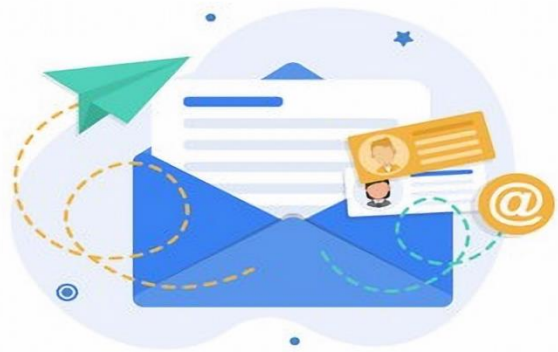
- You should deactivate various features of credit / debit card, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.



- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Cover the keypad with your other hand while entering the PIN at a POS site / ATM.

For E-mail account security

- Do not click on links sent through emails from unknown addresses / names.
- Avoid opening emails on public or free networks.
- Do not store secure credentials / bank passwords, etc., in emails.



For password security

- Use a combination of alphanumeric and special characters in your password.
- Keep two factor authentication for all your accounts, if such facility is available.
- Change your passwords periodically.
- Avoid having your date of birth, spouse name, car number etc. as passwords.





How do you know whether an NBFC accepting deposit is genuine or not?

- Verify whether the name of NBFC appears in the list of deposit taking NBFCs entitled to accept deposits, available at <https://rbi.org.in> and to ensure that it is not appearing in the list of companies prohibited from accepting deposits.
- NBFCs must prominently display the Certificate of Registration (CoR) issued by the Reserve Bank on its site / in its office. This certificate should also reflect that the NBFC has been specifically authorised by RBI to accept deposits. Scrutinize the certificate to ensure that the NBFC is authorised to accept deposits.
- NBFCs cannot accept deposits for a period less than 12-months and more than 60 months and the maximum interest rate that an NBFC can pay to a depositor should not exceed 12.5%.
- The Reserve Bank publishes the change in the interest rates on <https://rbi.org.in> → Sitemap → NBFC List → FAQs.





Precautions to be taken by depositors

- When depositing money, insist on a proper receipt for each and every deposit made with the bank / NBFC / company.
- The receipt should be duly signed by an officer authorised by the company and should state, *inter alia*, the date of the deposit, the name of the depositor, the amount in words and figures, rate of interest payable, maturity date and amount.
- In the case of brokers / agents, etc., collecting public deposits on behalf of NBFCs, verify that the brokers / agents are duly authorised for the purpose by the concerned NBFC.
- Remember that the Deposit Insurance facility is not available to depositors of NBFCs.





File a complaint

Complaint to RBI Ombudsman

- For filing complaints online, please visit the link at <https://cms.rbi.org.in/>
- Complaints in physical / paper form can be sent to CRPC, Reserve Bank of India, Central Vista, Sector -17, Chandigarh -160 017.

Complaint to Securities and Exchange Board of India (SEBI)

- Please visit the link at <https://www.sebi.gov.in/>

Complaint to Insurance Regulatory and Development Authority of India (IRDAI)

- Please visit the link at <https://www.irdai.gov.in/>

Complaint to National Housing Bank (NHB)

- Please visit the link at <https://nhb.org.in/>

Complaint to Cyber Police Station

- Please visit <https://cybercrime.gov.in/>



Glossary

- **Advance fee/Processing fee/Token fee:** These include preliminary payments such as documentation charges, meeting expenses, processing fees, other charges that may be applicable for disbursement of the loan to a borrower.
- **Two-factor authentication:** Authentication methodologies involve three basic 'factors'- something the user knows (e.g., password, PIN- either static or one time generated); something the user has (e.g., ATM/ smart card number, expiry date and CVV that is printed on the card); and something the user is (e.g., biometric characteristic, such as a fingerprint). Two-factor authentication (also known as 2FA) provides identification of users by means of a combination of two different components - what the user has and what the user knows/is to complete a transaction.
- **Authorisation:** The response from a card-issuing bank to a merchant's transaction authorisation request indicating that the payment information is valid and funds are available on the customer's credit card.
- **Card number:** The number assigned by a credit card association or card issuing bank to a card. This information must be provided to a merchant by a customer in order to make a credit card payment but should not be shared with anyone else. The string of digits is printed on the card.
- **Credit card:** A card that allows paying for products or services by availing unsecured/secured credit from a financial institution.
- **Credit limit:** The term refers to the maximum amount of credit a financial institution extends to a customer. A lending institution extends a credit limit on a credit card based on the analysis of the information given by the credit-seeking applicant. The credit limit can affect the customer's credit scores and their ability to obtain credit in the future.
- **CVV:** Stands for Card Verification Value. This is a 3-digit number printed on the card which is mandatory for completing most online transactions. These details are confidential and must NEVER be shared with anyone.
- **Debit card:** A card that allows paying for products or services by deduction of available funds in a bank account of the cardholder.



- **E-commerce platform:** It is a platform/website that enables buying and selling of goods and services including digital products over digital and electronic network.
- **EMI:** It stands for Equated Monthly Instalment. This a fixed monthly payment (includes principal and interest) to be made by a borrower to his lender/creditor (like bank/NBFC) each month till the loan/credit, along with interest, taken from the lender/creditor is paid off by the borrower in full.
- **Encryption:** The process of transforming processing information into an electronic code to maintain its secrecy.
- **Expiry date:** The date on which the validity of a card, contract, agreement, document, etc. expires. Transactions will be approved only in respect of cards or documents which have not yet expired.
- **Gateway:** It is an intermediary that provides technology infrastructure to route and facilitate processing of services such as transactions base management, risk management, etc. without its involvement directly. Payment Gateways are entities that provide technology infrastructure to route and facilitate processing of online payment transactions without any involvement in handling of funds.
- **Immediate payment services (IMPS):** It is an instant interbank electronic fund transfer service (up to a limit) through mobile phones, provided by National Payments Corporation of India (NPCI).
- **KYC:** Stands for Know Your Customer. It is process in which the financial institution makes an effort to verify the identity, suitability, and risks involved with maintaining a relationship with a customer by obtaining a set of documents and carrying out due diligence.
- **Money mule:** It is a term used to describe victims who are exploited by fraudsters into laundering stolen / illegal money via their bank account(s).
- **Multi-Level Marketing:** The practice of selling goods or services on behalf of a company in a system whereby participants receive commission on their sales as well as the sales of any participants they recruit.



- **National Automated Clearing House (NACH):** It is a centralised Electronic Clearing Service (ECS) system operated by National Payments Corporation of India (NPCI).
- **Near Field Communication (NFC):** It is a communication technology used to transmit data from a NFC equipped device to a capable terminal. The NFC technology is used to make a contactless payment that is carried out by keeping the smartphone/card near the NFC enabled machine.
- **National Electronic Fund Transfer (NEFT):** It is a nation-wide centralised payment system owned and operated by RBI, which enables bank customers in India to transfer funds between any two NEFT-enabled bank accounts.
- **OTP:** One Time Password is one of the factors in the authentication methodology, which the customer knows and is often used for carrying out online transactions. This is CONFIDENTIAL and should not be shared with anyone.
- **Phishing:** It refers to spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.
- **Point of Sale device (POS) / Acceptance Device (mPOS):** It refers to any device / terminal / machine installed at Merchant Establishments which enables the merchants to accept payments through payment cards (credit cards, debit cards, gift cards etc.).
- **Quick Response (QR) code:** The QR Code is type of a two-dimensional bar code. It consists of black squares arranged in a square grid on a white background. Imaging devices such as smartphone cameras can be used to read and interpret these codes. QR code contains information about the payee and is used to facilitate mobile payments at the point-of-sale by debiting the customers' account.
- **Remote Access:** It refers to luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.



- **UPI:** Unified Payment Interface is a platform that allows transfer of money from one bank / wallet account to other using a mobile phone which has access to the Internet. Once a customer registers for UPI with the bank, a unique virtual identifier is created and mapped to the customer's mobile phone to initiate the payment. It uses authentication in the form of UPI-PIN, which is CONFIDENTIAL and should not be shared with anyone.
- **Vishing:** It refers to phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers luring customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.
- **Wallet:** A wallet is like an account which can be used for purchase of goods and services against the stored value in it. A wallet can be virtual (e.g. mobile wallet) or physical (prepaid cards).



(22)

**Government of Arunachal Pradesh
Finance, Planning & Investment Department
(Economic Affairs Branch)
Itanagar.**

No. FIN/EA-25/2011(Vol-II) *378*

Dated Itanagar, the 2nd May, 2023.

To,

**The Secretary,
Department of Information Technology,
Govt. of Arunachal Pradesh,
Itanagar.**

Subject:- Awareness Programme on Financial Literacy – Regarding.

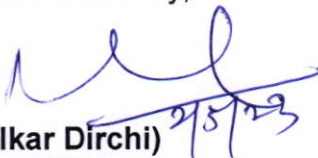
Sir,

With reference to the subject cited above, I am directed to share herewith a soft copy of a booklet '**BE(A)WARE** - A booklet on Modus Operandi of Financial Fraudsters' alongwith link <https://rbidocs.rbi.org.in/rdocs/content/PDFs/BEWARE07032022.pdf> for favour of your information and to request you to put up the material (booklet) on the Government Website for awareness of the public.

This is for favour of your information and necessary action please.

Enclosed: As stated above.

Yours Sincerely,



(Ikar Dirchi)
Joint Secretary (Finance)
Govt. of Arunachal Pradesh,
Itanagar.

Memo No. FIN/EA-25/2011(Vol-II)

Dated Itanagar, the 2nd May, 2023.

Copy for information to:-

1. The US to the Chief Secretary, Govt. of Arunachal Pradesh, Itanagar.
2. The PS to Principal Secretary (Finance), Govt. of Arunachal Pradesh, Itanagar.
3. All the Principal Secretaries/Commissioners/Secretaries, Govt. of Arunachal Pradesh for information.
4. The SPA to Secretary (Finance), Govt. of Arunachal Pradesh, Itanagar for information.
5. All Deputy Commissioner(s), Govt. of Arunachal Pradesh for information and necessary action.
6. All the Director(s)/Chief Engineer(s), Govt. of Arunachal Pradesh for information and necessary action.
7. Office copy.


(Ikar Dirchi)
Joint Secretary (Finance)
Govt. of Arunachal Pradesh,
Itanagar.

BE(A)WARE



**A BOOKLET
ON
MODUS OPERANDI
OF
FINANCIAL FRAUDSTERS**



RESERVE BANK OF INDIA





Table of Contents

	Subject	Page No.
	<u>Preface</u>	1
	<u>Part A - Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks</u>	2
1	<u>Phishing links</u>	3
2	<u>Vishing calls</u>	4
3	<u>Frauds using online sales platforms</u>	5
4	<u>Frauds due to the use of unknown / unverified mobile apps</u>	6
5	<u>ATM card skimming</u>	7
6	<u>Frauds using screen sharing app / Remote access</u>	8
7	<u>SIM swap / SIM cloning</u>	9
8	<u>Frauds by compromising credentials through search engines</u>	10
9	<u>Scam through QR code scan</u>	11
10	<u>Impersonation on social media</u>	12
11	<u>Juice jacking</u>	13
12	<u>Lottery frauds</u>	14
13	<u>Online job frauds</u>	15
14	<u>Money mules</u>	16
	<u>Part B - Modus Operandi and Precautions to be taken against Fraudulent Transactions - NBFCs</u>	17
1	<u>Fake advertisements for grant of loans</u>	18
2	<u>SMS / Email / Instant Messaging / Call scam</u>	19
3	<u>OTP based frauds</u>	20
4	<u>Fake loan websites / App frauds</u>	21
5	<u>Money circulation / Ponzi / Multi-Level Marketing (MLM) scheme frauds</u>	22
6	<u>Loans with forged documents</u>	23
	<u>Part C - General precautions to be taken for financial transactions</u>	24
	<u>Glossary</u>	32



Preface

There has been a surge in usage of digital modes of payment in the recent years. This gained further momentum during the Covid-19 induced lockdowns. While enhancing customer convenience, it also furthered the national objective of financial inclusion. However, as the speed and ease of doing financial transactions has improved, the number of frauds reported in retail financial transactions have also gone up. Fraudsters have been using innovative methods to defraud the common and gullible people of their hard-earned money, especially the new entrants in the use of digital platforms who are not entirely familiar with the techno-financial eco-system.

This booklet has been compiled from various incidents of frauds reported as also from complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are inexperienced, or not so experienced, in digital and electronic modes of financial transactions. The booklet is intended to create awareness among the members of public about the modus operandi adopted by fraudsters to defraud and mislead them, while also informing them about the precautions to be taken while carrying out financial transactions. It emphasizes the need for keeping one's personal information, particularly the financial information, confidential at all times, be-ware of unknown calls / emails / messages, practicing due diligence while performing financial transactions and changing the secure credentials / passwords from time to time. Hence the title **BE(A)WARE** – Be Aware and Beware!

This booklet is part of the public awareness initiative by the Consumer Education and Protection Department, Reserve Bank of India and has been conceptualized by the office of Ombudsman, Mumbai-II.



Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks





1. Phishing links

Modus Operandi

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.



Precautions

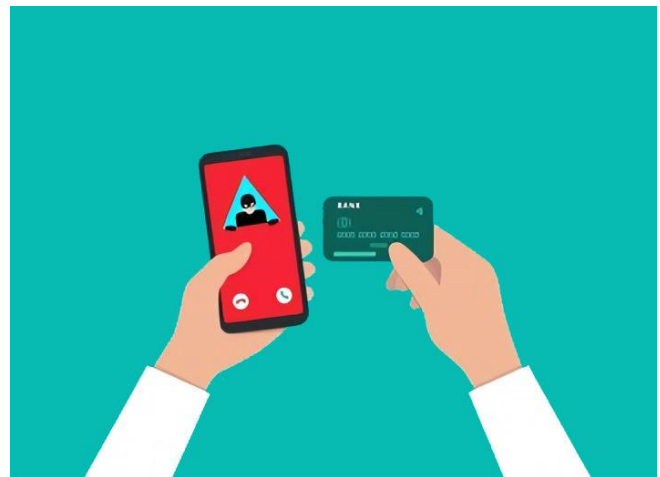
- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform



2. Vishing calls

Modus Operandi

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



Precautions

- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.



3. Frauds using online sales platforms

Modus Operandi

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is **no need to enter PIN / password** anywhere to **receive** money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.



4. Frauds due to the use of unknown / unverified mobile apps

Modus Operandi

- Fraudsters circulate through SMS / email / social media / Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before / after installation of such apps.



Precautions

- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.
- As a prudent practice before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.



5. ATM card skimming

Modus Operandi

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.



Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.



6. Frauds using screen sharing app / Remote access

Modus Operandi

- Fraudsters trick the customer to download a screen sharing app.
- Using such app, the fraudsters can watch / control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorised transfer of funds or make payments using the customer's Internet banking / payment apps.



Precautions

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.



7. SIM swap / SIM cloning

Modus Operandi

- Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.



Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.



8. Frauds by compromising credentials on results through search engines

Modus Operandi

- Customers use search engines to obtain contact details / customer care numbers of their bank, insurance company, Aadhaar updation centre, etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- Customers may end up contacting unknown / unverified contact numbers of the fraudsters displayed as bank / company's contact numbers on search engine.
- Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials / details for verification.
- Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.



Precautions

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- Please also note that customer care numbers are never in the form of mobile numbers.



9. Scam through QR code scan

Modus Operandi

- Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.
- By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.



Precautions

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.



10. Impersonation on social media

Modus Operandi

- Fraudsters create fake accounts using details of the users of social media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users' trust over a period of time. When the users share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.



Precautions

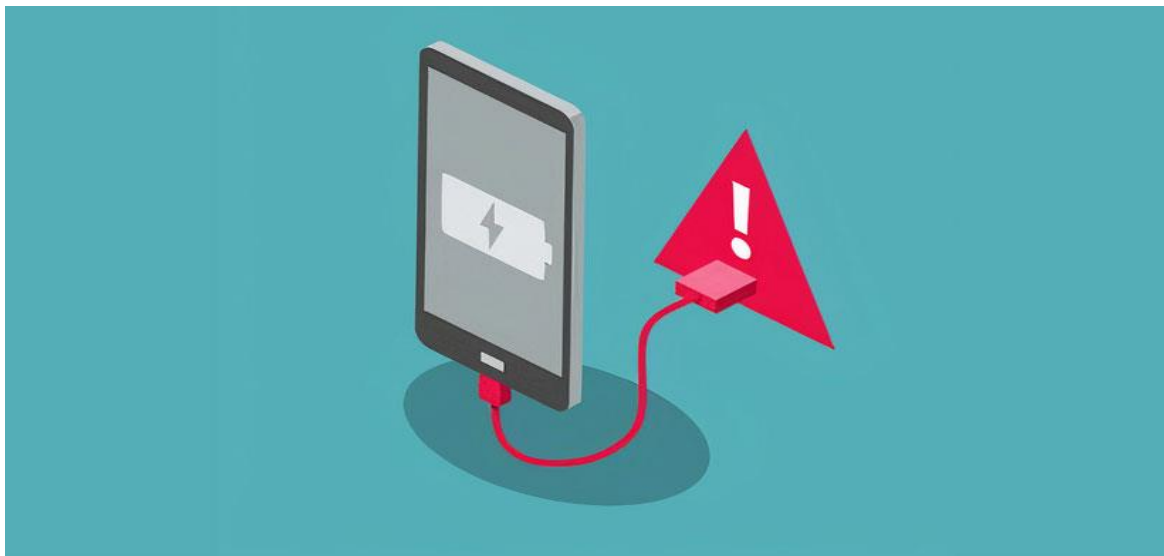
- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.



11. Juice jacking

Modus Operandi

- The charging port of a mobile, can also be used to transfer files / data.
- Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).



Precaution

- Avoid using public / unknown charging ports / cables.



12. Lottery fraud

Modus Operandi

- Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account / credit card details on a website from which data is captured by the fraudsters.
- Fraudsters also ask the customers to pay taxes/ forex charges / upfront or pay the shipping charges, processing / handling fee, etc., to receive the lottery / product.
- Fraudsters in some cases, may also pose as a representative of RBI or a foreign bank / company / international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.
- Since the requested money is generally a very small percentage of the promised lottery / prize, the customer may fall into the trap of the fraudster and make the payment.



Precautions

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.



13. Online job fraud

Modus Operandi

- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / credit card / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.



Precautions

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.



14. Money mules

Modus Operandi

- Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen / illegal money via their bank account/s.



- Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions.
- The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Alternatively, the fraudster may direct the money mule to withdraw cash and hand it over to someone.
- When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

Precautions

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee.
- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.



Modus Operandi and Precautions to be taken against Fraudulent Transactions – Non Banking Financial Companies (NBFCs)





1. Fake advertisements for extending loans by fraudsters

Modus Operandi

- Fraudsters issue fake advertisements offering personal loans at very attractive and low rates of interest or easy repayment options or without any requirement of collateral/ security, etc.
- Fraudsters send emails with such offers and ask the borrowers to contact them. To gain credibility with the gullible borrowers and to induce confidence, these email-ids are made to look-like the emails IDs of senior officials of well-known / genuine Non-Banking Financial Companies (NBFCs).
- When borrowers approach the fraudsters for loans, the fraudsters take money from the borrowers in the name of various upfront charges like processing fees, Goods and Services Tax (GST), intercity charge, advance Equated Monthly Instalment (EMI), etc., and abscond without disbursing the loans.
- Fraudsters also create fake website links to show up on search engines, when people search for information on loans.



Precautions

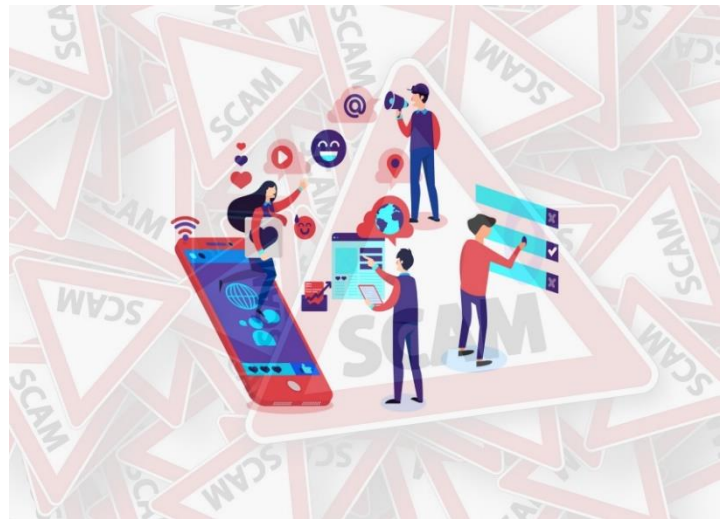
- Loan processing fee charged by NBFCs / banks is deducted from the sanctioned loan amount and not demanded upfront in cash from the borrower.
- Never pay any processing fee in advance as NBFCs / banks will never ask for an advance fee before the processing of loan application.
- Do not make payments or enter secure credentials against online offer of loans at low interest rates, etc., without checking / verifying the particulars through genuine sources.



2. SMS / Email / Instant Messaging / Call scams

Modus Operandi

- Fraudsters circulate fake messages in instant messaging apps / SMS / social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.
- The fraudsters may even share their Aadhaar card / Pan Card and fake NBFC ID card.
- After sending such bulk messages / SMS / emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.



Precautions

- Never believe loan offers made by people on their own through telephones / emails, etc.
- Never make any payment against such offers or share any personal / financial credentials against such offers without cross-checking that it is genuine through other sources.
- Never click on links sent through SMS / emails or reply to promotional SMS / emails.
- Never open / respond to emails from unknown sources containing suspicious attachment or phishing links.



3. OTP based Frauds

Modus Operandi

- Fraudsters impersonating as NBFCs, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number.
- When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.



Precautions

- Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.
- Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.
- Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications.

Modus Operandi

-
- A collection of 12 isometric illustrations arranged in a grid-like fashion. Each illustration features a central figure dressed in a purple hooded robe and a black mask, representing a hacker. The figure is shown in various poses of interaction with digital technology: sitting on a red chair using a laptop, standing and holding a smartphone, holding a yellow shield, standing next to a large smartphone displaying a document, standing on a stack of yellow coins, standing on a smartphone displaying a globe, standing on a smartphone displaying a network diagram, standing on a smartphone displaying a padlock, standing on a smartphone displaying a skull and crossbones, and standing on a desktop computer. The background is a solid light blue.

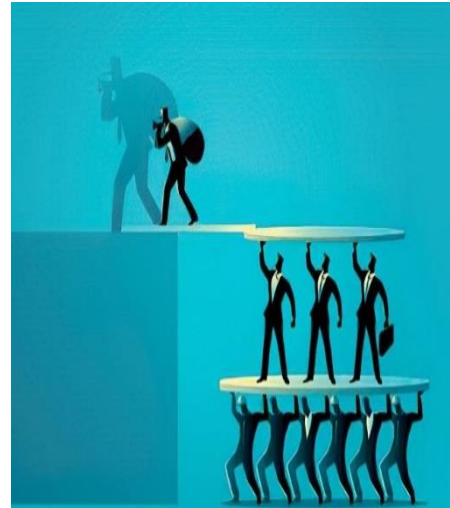
- Verify if the lender is registered with the Government / Regulator /authorised agencies
- Check whether the lender has provided a physical address or contact information to ensure it is not difficult to contact them later.
- Beware if the lender appears more interested in obtaining personal details rather than in checking credit scores.
- Remember that any reputed NBFC / bank will never ask for payment before processing the loan application.
- Genuine loan providers never offer money without verifying documents and other credentials of the borrowers.
- Verify if these NBFC-backed loan apps are genuine.



5. Money circulation / Ponzi / Multi-Level Marketing (MLM) schemes fraud

Modus Operandi

- Fraudsters use MLM / Chain Marketing / Pyramid Structure schemes to promise easy or quick money upon enrolment / adding of members.
- The schemes not only assure high returns but also pay the first few instalments (EMIs) to gain confidence of gullible persons and attract more investors through word of mouth publicity.
- The schemes encourage addition of more people to the chain / group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.
- This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.



Precautions

- Returns are proportional to risks. Higher the return, higher is the risk.
- Any scheme offering abnormally high returns (40-50% p a) consistently, could be the first sign of a potential fraud and caution needs to be exercised.
- Always notice that any payment / commission / bonus / percentage of profit without the actual sale of goods / service is suspicious and may lead to a fraud.
- Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing / Chain Marketing / Pyramid Structure schemes.
- Acceptance of money under Money Circulation / Multi-level Marketing / Pyramid structures is a cognizable offence under the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- In case of such offers or information of such schemes, a complaint must be immediately lodged with the State Police.



6. Fraudulent loans with forged documents

Modus Operandi

- Fraudsters use forged documents to avail services from financial institutions.
- Fraudsters commit identity thefts, steal personal information of customers such as identity cards, bank account details etc., and use this information or credentials to avail benefits from a financial institution.
- Fraudsters pose as NBFC employees and collect KYC related documents from customers.



Precautions

- Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.
- Such documents should be shared only with the entity's authorised personnel or on authorised email IDs of the entities.
- Follow up with the concerned entities to ensure that the documents shared by you are purged immediately by them in case of non-sanction of loan and/ or post closure of the loan account.



General Precautions to be taken for financial transactions





General precautions

- Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (<https://> - URL with a pad lock symbol) before making online payments / transactions.
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites / devices / public laptop / desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.



For device / computer security

- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Always scan unknown Universal Serial Bus (USB) drives / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices.





For safe internet browsing

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.

For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.





Factors indicating that a phone is being spied

- Unfamiliar applications are being downloaded on the phone.
- There is a faster than usual draining of phone battery.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.
- An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background.
- Spyware apps might sometimes interfere with a phone's shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.
- Note that text messages can be used by spyware and malware to send and receive data.

Actions to be taken after occurrence of a fraud

- Block not only the debit card / credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the **official customer care number** available on the bank's website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.
- Dial helpline number 155260 or 1930 or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in).
Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile.

Precautions related to Debit / Credit cards

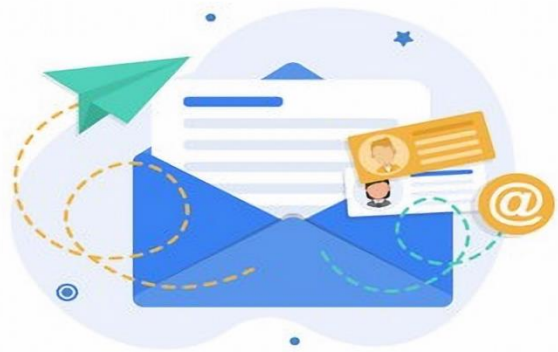
- You should deactivate various features of credit / debit card, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.



- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Cover the keypad with your other hand while entering the PIN at a POS site / ATM.

For E-mail account security

- Do not click on links sent through emails from unknown addresses / names.
- Avoid opening emails on public or free networks.
- Do not store secure credentials / bank passwords, etc., in emails.



For password security

- Use a combination of alphanumeric and special characters in your password.
- Keep two factor authentication for all your accounts, if such facility is available.
- Change your passwords periodically.
- Avoid having your date of birth, spouse name, car number etc. as passwords.





How do you know whether an NBFC accepting deposit is genuine or not?

- Verify whether the name of NBFC appears in the list of deposit taking NBFCs entitled to accept deposits, available at <https://rbi.org.in> and to ensure that it is not appearing in the list of companies prohibited from accepting deposits.
- NBFCs must prominently display the Certificate of Registration (CoR) issued by the Reserve Bank on its site / in its office. This certificate should also reflect that the NBFC has been specifically authorised by RBI to accept deposits. Scrutinize the certificate to ensure that the NBFC is authorised to accept deposits.
- NBFCs cannot accept deposits for a period less than 12-months and more than 60 months and the maximum interest rate that an NBFC can pay to a depositor should not exceed 12.5%.
- The Reserve Bank publishes the change in the interest rates on <https://rbi.org.in> → Sitemap → NBFC List → FAQs.





Precautions to be taken by depositors

- When depositing money, insist on a proper receipt for each and every deposit made with the bank / NBFC / company.
- The receipt should be duly signed by an officer authorised by the company and should state, *inter alia*, the date of the deposit, the name of the depositor, the amount in words and figures, rate of interest payable, maturity date and amount.
- In the case of brokers / agents, etc., collecting public deposits on behalf of NBFCs, verify that the brokers / agents are duly authorised for the purpose by the concerned NBFC.
- Remember that the Deposit Insurance facility is not available to depositors of NBFCs.





File a complaint

Complaint to RBI Ombudsman

- For filing complaints online, please visit the link at <https://cms.rbi.org.in/>
- Complaints in physical / paper form can be sent to CRPC, Reserve Bank of India, Central Vista, Sector -17, Chandigarh -160 017.

Complaint to Securities and Exchange Board of India (SEBI)

- Please visit the link at <https://www.sebi.gov.in/>

Complaint to Insurance Regulatory and Development Authority of India (IRDAI)

- Please visit the link at <https://www.irdai.gov.in/>

Complaint to National Housing Bank (NHB)

- Please visit the link at <https://nhb.org.in/>

Complaint to Cyber Police Station

- Please visit <https://cybercrime.gov.in/>



Glossary

- **Advance fee/Processing fee/Token fee:** These include preliminary payments such as documentation charges, meeting expenses, processing fees, other charges that may be applicable for disbursement of the loan to a borrower.
- **Two-factor authentication:** Authentication methodologies involve three basic 'factors'- something the user knows (e.g., password, PIN- either static or one time generated); something the user has (e.g., ATM/ smart card number, expiry date and CVV that is printed on the card); and something the user is (e.g., biometric characteristic, such as a fingerprint). Two-factor authentication (also known as 2FA) provides identification of users by means of a combination of two different components - what the user has and what the user knows/is to complete a transaction.
- **Authorisation:** The response from a card-issuing bank to a merchant's transaction authorisation request indicating that the payment information is valid and funds are available on the customer's credit card.
- **Card number:** The number assigned by a credit card association or card issuing bank to a card. This information must be provided to a merchant by a customer in order to make a credit card payment but should not be shared with anyone else. The string of digits is printed on the card.
- **Credit card:** A card that allows paying for products or services by availing unsecured/secured credit from a financial institution.
- **Credit limit:** The term refers to the maximum amount of credit a financial institution extends to a customer. A lending institution extends a credit limit on a credit card based on the analysis of the information given by the credit-seeking applicant. The credit limit can affect the customer's credit scores and their ability to obtain credit in the future.
- **CVV:** Stands for Card Verification Value. This is a 3-digit number printed on the card which is mandatory for completing most online transactions. These details are confidential and must NEVER be shared with anyone.
- **Debit card:** A card that allows paying for products or services by deduction of available funds in a bank account of the cardholder.



- **E-commerce platform:** It is a platform/website that enables buying and selling of goods and services including digital products over digital and electronic network.
- **EMI:** It stands for Equated Monthly Instalment. This is a fixed monthly payment (includes principal and interest) to be made by a borrower to his lender/creditor (like bank/NBFC) each month till the loan/credit, along with interest, taken from the lender/creditor is paid off by the borrower in full.
- **Encryption:** The process of transforming processing information into an electronic code to maintain its secrecy.
- **Expiry date:** The date on which the validity of a card, contract, agreement, document, etc. expires. Transactions will be approved only in respect of cards or documents which have not yet expired.
- **Gateway:** It is an intermediary that provides technology infrastructure to route and facilitate processing of services such as transactions base management, risk management, etc. without its involvement directly. Payment Gateways are entities that provide technology infrastructure to route and facilitate processing of online payment transactions without any involvement in handling of funds.
- **Immediate payment services (IMPS):** It is an instant interbank electronic fund transfer service (up to a limit) through mobile phones, provided by National Payments Corporation of India (NPCI).
- **KYC:** Stands for Know Your Customer. It is a process in which the financial institution makes an effort to verify the identity, suitability, and risks involved with maintaining a relationship with a customer by obtaining a set of documents and carrying out due diligence.
- **Money mule:** It is a term used to describe victims who are exploited by fraudsters into laundering stolen / illegal money via their bank account(s).
- **Multi-Level Marketing:** The practice of selling goods or services on behalf of a company in a system whereby participants receive commission on their sales as well as the sales of any participants they recruit.



- **National Automated Clearing House (NACH):** It is a centralised Electronic Clearing Service (ECS) system operated by National Payments Corporation of India (NPCI).
- **Near Field Communication (NFC):** It is a communication technology used to transmit data from a NFC equipped device to a capable terminal. The NFC technology is used to make a contactless payment that is carried out by keeping the smartphone/card near the NFC enabled machine.
- **National Electronic Fund Transfer (NEFT):** It is a nation-wide centralised payment system owned and operated by RBI, which enables bank customers in India to transfer funds between any two NEFT-enabled bank accounts.
- **OTP:** One Time Password is one of the factors in the authentication methodology, which the customer knows and is often used for carrying out online transactions. This is CONFIDENTIAL and should not be shared with anyone.
- **Phishing:** It refers to spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.
- **Point of Sale device (POS) / Acceptance Device (mPOS):** It refers to any device / terminal / machine installed at Merchant Establishments which enables the merchants to accept payments through payment cards (credit cards, debit cards, gift cards etc.).
- **Quick Response (QR) code:** The QR Code is type of a two-dimensional bar code. It consists of black squares arranged in a square grid on a white background. Imaging devices such as smartphone cameras can be used to read and interpret these codes. QR code contains information about the payee and is used to facilitate mobile payments at the point-of-sale by debiting the customers' account.
- **Remote Access:** It refers to luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.



- **UPI:** Unified Payment Interface is a platform that allows transfer of money from one bank / wallet account to other using a mobile phone which has access to the Internet. Once a customer registers for UPI with the bank, a unique virtual identifier is created and mapped to the customer's mobile phone to initiate the payment. It uses authentication in the form of UPI-PIN, which is CONFIDENTIAL and should not be shared with anyone.
- **Vishing:** It refers to phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers luring customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.
- **Wallet:** A wallet is like an account which can be used for purchase of goods and services against the stored value in it. A wallet can be virtual (e.g. mobile wallet) or physical (prepaid cards).

