BE(A)WARE

A BOOKLET ON MODUS OPERANDI OF FINANCIAL FRAUDSTERS

OFFICE OF THE RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

Table of Contents

Preface

There has been a sizable surge in usage of digital modes of payment during the recent years. This has not only led to improved customer convenience, but also contributed to achievement of national objective of financial inclusion to a great extent. As the ease of doing financial transactions improved, the number of frauds in retail financial transactions have gone up. Fraudsters have been using innovative methods to defraud the hard-earned money of common and gullible people, especially new entrants who are not entirely familiar with the techno-financial eco-system.

In compiling this booklet, the sole objective has been to pack between its covers maximum possible extent of practical information of real value, especially for those who are inexperienced in financial transactions. It is not just a collection of incidents, gathered at random from various sources, but a meticulously compiled document from the variety of complaints received at offices of Banking Ombudsman. This booklet is an attempt at creating awareness among public about the modus operandi of the fraudsters, while also providing some inputs about precautions to adopt while carrying out financial transactions. This booklet emphasizes the need to keep one's personal information safe, beware of unknown calls/emails, 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 building initiative by this Office.

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

1. Phishing Links

Modus Operandi

- Fraudsters create a third-party website which looks like existing genuine website, such as bank's website or e-commerce website or search engine, etc.
- These links are generally circulated by fraudsters through SMS / social media / email / Instant Messenger, etc.
- Most of the time, customers enter secure credentials by just having a glance and clicking at the link but not checking the detailed URL.
- The links are masked through authentic looking names of websites, but in reality, the customer gets redirected to phishing website.
- When customers enter secure credentials on these websites, the same is captured and used by the fraudsters.

Precaution

One should not click unknown links and should delete the SMS / email immediately to avoid accessing them in future. Care should be taken to verify the website details especially where it requires entering financial credentials.

2. Vishing Calls

Modus Operandi

- Imposters call or approach the customers through telephone call / social media as bankers / company executives / insurance agents / government officials, etc., and seek confirmation of the secure credentials by sharing few details such as name or date of birth to gain confidence.

- In some cases, the imposters pressurize / trick customers into urgently / immediately sharing confidential details citing emergency, details required to block transaction, payment required to stop penalty, get attractive discount, etc. These credentials are then used to defraud the customers.

Precaution

Bank officials / financial institutions / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.

3. Frauds using Online Selling platforms

Modus Operandi

- Fraudsters pretend to be buyers on online selling platform & show interest in your product.
- Instead of paying money to you, they use “request money” option through UPI app and insist to approve the request to pull money from your bank account.

Precaution

- One should be careful while making financial transactions for online products.
- Always remember, to receive money there is no need to enter your PIN / password anywhere.
- If UPI or any other app asks you to enter your PIN to complete transaction, it means you will end up sending money instead of receiving it.

4. Frauds due to use of Unknown / Unverified Mobile Apps

Modus Operandi

- Fraudsters gain access to your mobile device / laptop / desktop once you download unknown / unverified mobile apps.
- These application links are generally shared through SMS / social media / Instant Messenger, etc. The links are masked through authentic looking names but in reality customer is redirected to download unknown application.
- Once the malicious application is downloaded, the fraudster can gain complete access to the device.

Precaution

Never download application from unverified / unknown sources.

5. ATM card skimming

Modus Operandi

- It has been observed that fraudsters install skimming devices in ATM machines & steal data from your card.
- PIN is also captured by installing dummy keypad, small / pinhole camera which is well-hidden from plain sight.
- Sometimes, fraudsters pretend to be other customers standing near-by and gain access to your PIN while you enter it.
- This data is then used to create duplicate card and withdraw amount from customer's account.

Precaution

- Verify to ensure that there is no extra device attached near card insertion slot or keypad of ATM machine while making transaction.
- Cover the keypad with your hand while entering your PIN.
- Do NOT enter the PIN in the presence of any other person standing close to you or share the card with anyone.

6. Frauds using Screen Sharing App / Remote Access

Modus Operandi

- Fraudsters trick you to download screen sharing apps through which they can watch / control your mobile / laptop to gain access to your financial credentials.
- Later they make payments using your Internet banking / payment apps.

Precaution

Do not download or activate share screen share feature with unknown people.

7. SIM Swap / SIM Cloning

Modus Operandi

- As most of the account details & authentication is connected to your registered mobile number, fraudsters try to gain access to the SIM card or obtain duplicate SIM card for carrying out digital transactions using OTP received on such duplicate SIM.
- The fraudsters generally call the customer by posing as a telephone / mobile network staff requesting details for providing free upgrade of SIM card from 3G to 4G or to provide additional benefit on SIM card.

Precaution

- Never share credentials pertaining to SIM card.
- You should immediately get suspicious, if you don't have mobile network in your phone for considerable time in a regular environment and contact Mobile operator to ensure that no duplicate SIM is being issued for your SIM.

8. Frauds by compromising credentials on results through Search Engines

Modus Operandi

- It has been observed that customers use search engines for obtaining contact details of their bank, insurance company, Aadhar updation centres, etc., and may end up contacting unknown / unverified contact numbers displayed on search engine.
- These contact details on search engines are often camouflaged by fraudsters to attract their victims towards them.
- Once the customers call them, the imposters ask the customers to give their card credentials / details for verification.
- Assuming this contact to be genuine, people compromise all their secure details & thus fall prey to frauds.

Precaution

Avoid searching for customer care contact details on search engine. These are often camouflaged by fraudsters. One should always look for official websites of Banks / companies to get contact details.

9. Scam through QR scan

Modus Operandi

Fraudsters often contact customers under various pretext and trick them into scanning QR codes using payment apps. This allows the fraudsters to withdraw money from customer's account.

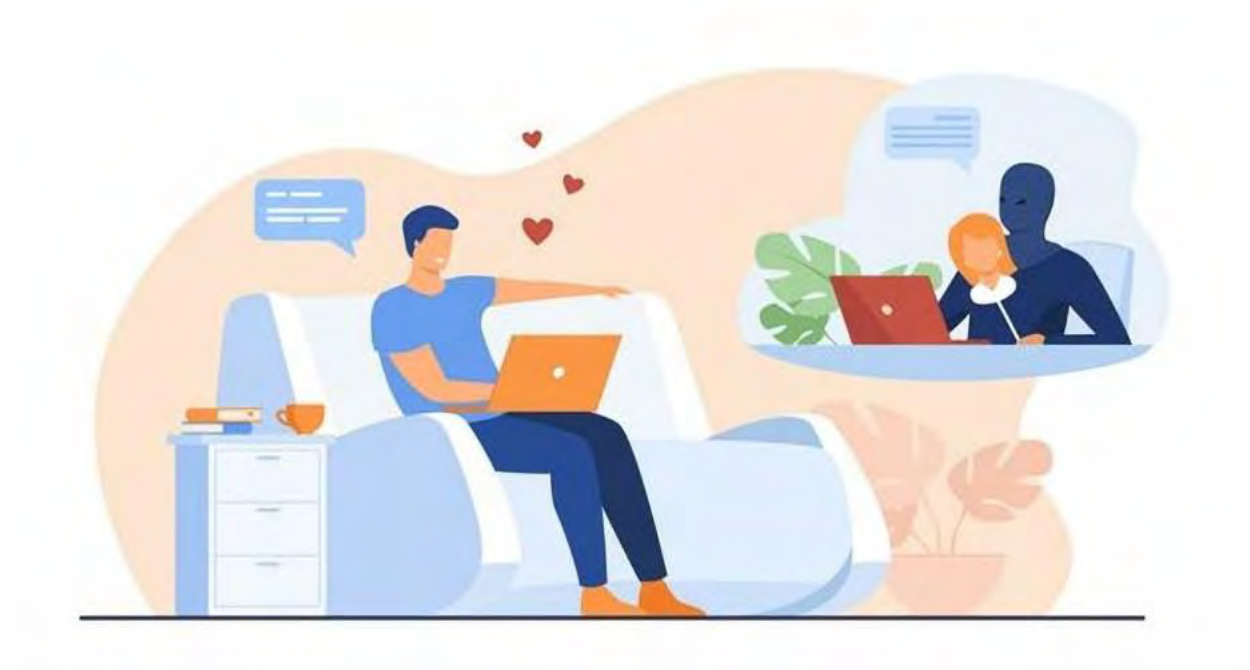
Precaution

Be cautious while scanning any QR codes using payment apps. QR codes have embedded account details in them to transfer amount to particular account.

10. Impersonating through Social Media

Modus Operandi

- Fraudsters create fake account on popular social media platforms like Facebook and Instagram. They send a request to your friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters also gain trust over a period of time and use the private information for extortion or blackmail later.



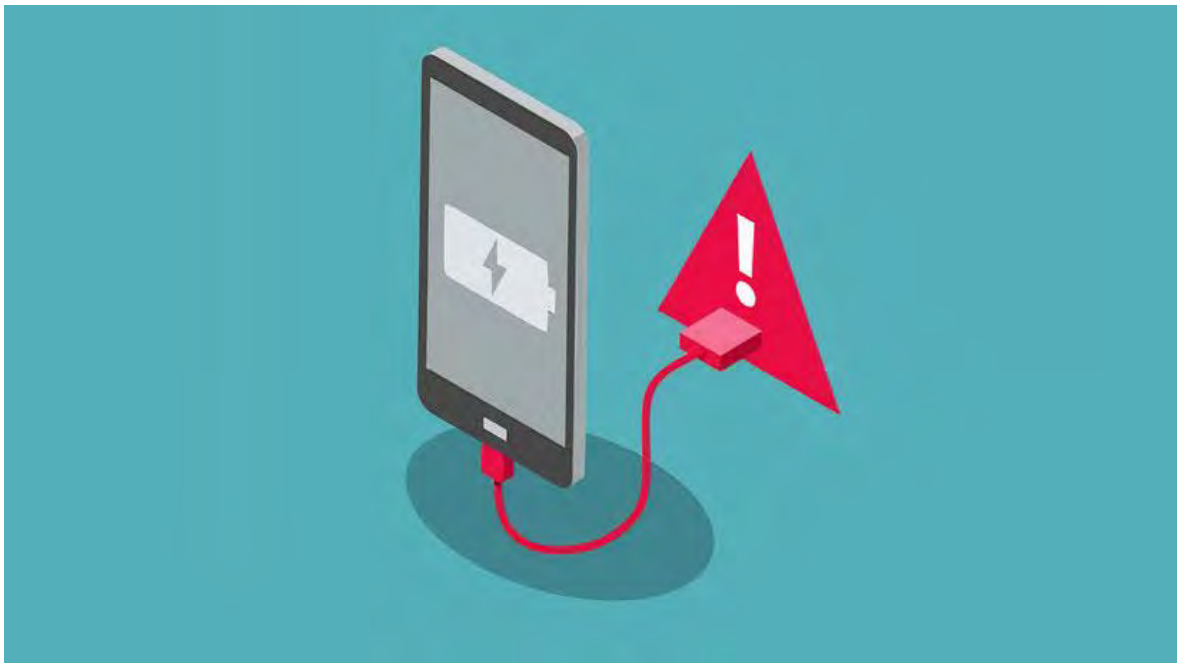
Precaution

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

11. Juice Jacking

Modus Operandi

- The charging port of a mobile, can also be used for transfer of files / data.
- Juice jacking is a type of cyber stealing, where, once your mobile is connected to unknown / unverified charging ports, unknown apps / malware are installed with which, the fraudsters can control / access / steal sensitive data, email, SMS, saved passwords.



Precaution

Always avoid using public / unknown charging ports / cables.

12. Lottery Fraud

Modus Operandi

- Fraudsters send email or make phone call that you have just won a huge lottery. However, in order to receive the money, it is required to confirm identity by verifying through bank account / credit card on their website from which data is captured.
- In some cases, the fraudsters ask to pay taxes upfront or pay the shipping charges, processing fee, etc., to receive the lottery / product.
- Since the requested money is very small percentage of the lottery / prize, the victim may fall into the trap of the fraudster and make payment.

Precaution

Do not make payments or share secure credentials for lottery calls / emails. Always doubt when you come across such unbelievable lottery or offers.

13. Online Job Fraud

Modus Operandi

- Fake job search portals are created and when victim shares secure credentials of bank account / credit card / debit card on these websites for registration, the account is compromised.
- In some cases, the fraudsters pose themselves as officials of a reputed company and confirm selection after doing fake interviews. The victim is incited into making payment for mandatory training program, etc.

Precaution

- Always remember that a genuine company offering job will never ask for money.
- Do not make payments on unknown job portals.

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

1. Fake Advertisements for Extending Loan by Fraudsters

- Fraudsters issue fake advertisements of personal loan offers at very attractive low rates of interest or with easy repayment options or without any security requirement, etc., and ask the customers to contact them.
- To gain credibility of gullible customers and to induce confidence, these email-ids would be look-alike emails IDs of senior officials of well-known / genuine NBFCs.
- When customers approach the fraudsters for loans, the fraudsters take various upfront charges like processing fee, GST, intercity charge, advance EMI, un-hold charges, etc., and abscond without disbursing the loans.
- Fraudsters also create fake website links to show up on search engines which people search to find out about loans, etc.

Precaution

- ✓ NBFC/Banker will never ask for an advance fee before the processing of loan application.
- ✓ Banks / NBFCs charge a processing fee, which is deducted from the loan amount.
- ✓ Do not make payments or enter secure credentials against online offer of loans at low interest, etc., without checking the particulars through genuine sources.

2. SMS / Email / Instant Messaging / Call Scam

- Fraudsters circulate fake messages in Instant messenger / SMS / social media regarding availability of 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 even share their Aadhaar card / Pan Card and fake NBFC ID card.
- After sending such bulk messages / SMS /email to loan seekers, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the victims pay these charges, the fraudsters abscond with the money, leaving the victim with very little chance of getting it back.

Precaution

- ✓ 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.
- ✓ 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.

3. OTP based Fraud

- Victims get SMS / Instant messages from fraudsters impersonating as NBFCs offering loans or enhancement of credit limit and are asked to contact the fraudster's mobile number.
- When the victims call the number, the fraudsters ask them to fill few forms (even online) containing financial details and they incite / convince them to share the OTP or PIN details, resulting in loss of money.

Precaution

- Never share OTP / PIN Numbers / personal details, etc., in any form with anyone.
- Regularly check SMS / emails to ensure that no OTP is generated without your knowledge.

4. Fake Loan websites / App Frauds

- There are many unscrupulous loan apps which offer instant and short-term loan. These apps dupe the borrowers and may also charge significantly higher interest rates.
- To attract gullible customers, the fraudsters advertise "limited period offers" and ask applicants to make urgent decisions using scareware tactics.

Precaution

Check the following points before taking loan from dubious loan app, etc.

- ✓ Is the lender more interested in knowing personal details rather than checking credit scores?
- ✓ Is the lender registered with the Government / authorised agencies?
- ✓ Check whether the lender has provided a physical address or contact information; otherwise it may be difficult to contact them at a later point.
- ✓ Remember any reputed NBFC / Bank will never ask for payment before processing the loan application.
- ✓ Genuine loan providers never offer money without verifying documents.
- ✓ Verify if these NBFC-backed loan apps are genuine.

5. Money Circulation/Ponzi/Multi-Level Marketing (MLM) Schemes Fraud

- MLM / Chain Marketing / Pyramid Structure schemes promise easy or quick money upon enrolment / adding of members.
- The schemes not only assure high returns but also pay the first few instalments as promised to gain confidence of gullible persons and attract more investors through word of mouth publicity.
- The Schemes encourage to add more and more people to join the chain / group, for which commission is paid to enroller, rather than commission from the sale of products.
- Due to this model, the scheme becomes unsustainable after some time when number of people joining the scheme starts reducing. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people.

PRECAUTION: while making investment in Ponzi/MLM Schemes

- ✓ Returns are proportional to risks. Higher the return, higher is the risk. So, if any scheme is offering abnormally (say 40-50 per cent every year) high returns consistently, it is the first sign of potential fraud and to exercise caution.
- ✓ 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.
- ✓ Public should 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 Chit and Money Circulation (Banning) Act 1978. Members of public coming across such offers should immediately lodge a complaint with the State Police.

6. Fraudulent Loans with Forged Documents

- The forged documents frauds are frauds in which a person or an entity uses forged documents for availing any form of services from financial institutions.
- Such frauds happen while sharing the KYC related documents with the entities without verifying the authenticity of the NBFC employee / the authenticity of the NBFC's email id.
- Fraud loans are also sanctioned based on identity thefts by stealing personal information of the victims such as identity cards, bank account details, etc., and using this information or credentials for availing benefits from a financial institution.

Precaution

- ✓ The customers while availing loan from any entity should be vigilant while providing the KYC and other personal documents including the NACH form post disbursement of loan.
- ✓ Such documents should be shared only with the entity's authorized personnel or authorized email IDs of the entities.
- ✓ Also, on non-sanction of loan and post closure of the loan, the customer should invariably request the entities for purging of documents given by the customer to the entities.

General Precautions to be taken for Financial Transactions

General

- Be wary of suspicious looking pop ups that appear during your browsing session.
- Always check for a secure payment gateway (https:// - URL with a Pad Lock Symbol) before making online payments.
- Keep your PIN (Personal Identification Number), password, and credit or debit card number, CVV private.
- Avoid saving card details on websites/devices/public laptop/desktops.
- Turn on two-factor authentication where facility is available.
- Never open emails from unknown sources containing 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 the device and install updates whenever available.
- Always scan unknown USB drives / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after specified time.
- Do not install unknown applications or software.
- Do not store passwords or confidential information on unknown devices.

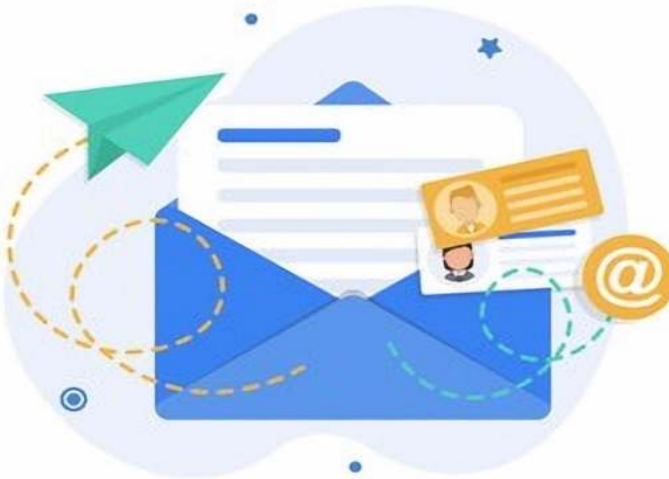
For Safe Internet Browsing

- Avoid visiting unsecured websites.
- Avoid using unknown browsers.
- Avoid saving passwords on public devices.
- Avoid entering secure credentials on unknown websites.
- Do not share private information to unknown persons on social medial.
- Always verify security of the page, in case an email or SMS link is redirected.

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 periodic basis.
- Do not use same passwords for email and internet banking.
- Avoid using public terminals (viz. cyber café, etc.) for financial transactions.

For E-mail Account Security



- Do not click emails from unknown addresses.
- Avoid using 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 authentications for all your accounts if facility is available.
- Change passwords periodically.

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

- The depositor should verify whether the NBFC is present in the list of deposit taking NBFCs entitled to accept deposits, available at https://rbi.org.in and 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. This certificate should also reflect that the NBFC has been specifically authorized by RBI to accept deposits. Depositors must scrutinize the certificate to ensure that the NBFC is authorized to accept deposits.
- NBFCs cannot accept deposit for a period less than 12-month 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.

Precaution to be taken by depositors

- The depositor must insist on a proper receipt for every amount of deposit placed with the company.
- The receipt should be duly signed by an officer authorized by the company and should state 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, the depositors should satisfy themselves that the brokers/agents are duly authorized by the NBFC.
- The depositor must bear in mind that Deposit Insurance facility is not available to depositors of NBFCs.

How to Make an Online Complaint

Complaint to RBI

- Please visit the link at https://cms.rbi.org.in/

Complaint to SEBI

- Please visit the link at https://scores.gov.in/

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

- Please visit the link at https://igms.irda.gov.in/

Complaint to National Housing Bank (NHB)

- Please visit the link at https://grids.nhbonline.org.in/

Complaint to Cyber Police Station

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

****

Glossary*

- **Advance fee/Processing Fee/Token fee**: It means all such initial payments which shall not be limited to documentation reimbursement, meeting expenses, applicable processing fees and any other applicable charges as may be levied for disbursal of the loan to the borrower.
- **Two-Factor Authentication:** Two-factor authentication (also known as 2FA) provides unambiguous identification of users by means of the combination of two different components, what you have – Card (number, expiry date and CVV that is printed on the card), what you know – PIN (either static or One time generated) to validate.
- **3-D Secure:** 3-D Secure is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions. It is also known as Verified by Visa, MasterCard Secure Code or American Express SafeKey.
- **Acquiring Bank:** An acquiring bank is a bank that processes credit or debit cards. Acquiring bank usually supports multiple card schemes such as Visa, MasterCard, Maestro and RuPay.
- **Authorisation:** The response from a card-issuing bank to a merchant's transaction authorization request indicating that payment information is valid and funds are available on the customer's credit card.
- **Bank Identification Number (BIN):** An identification number assigned by Visa and MasterCard to each of its member financial institutions, banks and processors.
- **BIN Validation:** Process of checking the BIN of the card against the participating BIN list
- **Blacklisting**: The practice of collecting information to detect deceitful buyers or high-risk merchants with the purpose of preventing frauds.

(*Source-Internet and other publications)

- **Card capture page**
- Secure page on which card details are captured. Entities that have PCI DSS certification are allowed to capture card details. Examples of entities that have a card capture page.
- Acquiring Bank (e.g., SBI, HDFC)
- Aggregator (e.g., PayU)
- Merchant (e.g., Flipkart, Amazon)
- **Card Number**
    - The account number assigned by a credit card association or card issuing bank to a cardholder. This information must be provided to a merchant by a customer in order to make a credit card payment.
    - The string of digits printed on the front of the card (these digits signifies band identification number, category, currency, etc.)
    - Visa, MasterCard, Maestro, RuPay: 16 digits
    - Amex: 15 digits
- **Card Present (CP):** During the transaction, the cardholder or card is present at the point of sale Example: Card swipe done at grocery store. Usually TDR/MDR in CP cases are lower than Card Not Present (CNP) cases as risk is lower in CP transactions (rates are adjusted for risks).
- **Card Vaulting:** Process of storing the card details (card number and CVV) and show the stored card details during subsequent transactions Card can be stored by PCI DSS certified entity (acquiring bank, aggregator or merchant).
- **Closed-loop prepaid cards/wallet:** Cards/wallet that can be used at only one merchant and funds cannot be withdrawn to source account or through ATM.
- **Co-branded cards:** Cards that are issued by a financial institution with a card scheme and has corporate branding.
- **Collection account:** The bank account of the merchant to which proceeds of the payment gateway is credited. The collection account can be a current account, nodal account, or escrow account.

- **Credit Cards:** The cards that allow paying for products or services by borrowing money from a financial institution.
- **Chargeback**
  - A dispute raised by credit cardholder with issuing bank.
  - There can be various reasons for a chargeback to take place:
    - Service/product not delivered
    - upon cancellation refund is not issued
    - suspected fraudulent transactions
    - Card being hacked
  - In such circumstances, the issuing bank will send the chargeback to acquirer bank and acquiring bank reaches out to merchant directly (if acquiring bank has direct integration with merchant) or through aggregator (if transaction is processed through aggregator) to provide proof to support delivery or refund within stipulated time else chargeback will be considered valid and merchant will be obliged to return chargeback amount.
- **Credit limit:** The term credit limit refers to the maximum amount of credit a financial institution extends to a client. A lending institution extends a credit limit on a credit card or a line of credit. Lenders usually set credit limits based on the information given by the credit-seeking applicant. A credit limit is a factor that affects consumers' credit scores and can impact their ability to obtain credit in the future.
- **CVV** - Stands for Card Verification Value. This number is vital for completing online transactions and should never be shared with anyone.
- **Debit Cards:** The cards that work through the automatic deduction of available funds in a bank account to make a purchase.
- **Declined Payments:** Transactions that are not approved by the card-issuing bank are marked as declined. No further action may be taken for declined transactions and customer has to retry to make payment.

Digital Signature: An electronic file containing unique information that is used to verify the trustworthiness of an organization or individual. Digital Certificates are issued by a Certificate Authority and are used with the Secure Sockets Layer (SSL) protocol.

- **E-commerce Platform:** Software that provides various functionalities that are required to run an eCommerce business such as website, category management, pricing management, order management and payment management. For example – Shopify, Magento and others.
- **EMI (Equated Monthly Instalments)**
  - A provision is given by a bank to the cardholder (customer) to split the transaction amount to a smaller amount that is payable on a monthly basis. For this service, bank may charge a processing fee or interest.
- **EMV:** EuroPay, MasterCard and Visa, is a microchip-based technology designed to reduce fraud at the point-of-sale.
- **Encryption:** The process of transforming processing information to make it unusable to anyone except those possessing special knowledge usually referred to as a key.
- **Expiry Date:** The date on which the validity of a card expires. Transactions will only be approved for cards that are not yet expired.
- **Flat Fee:** Transaction charges are per transaction and not the percentage of the transaction amount.
- **Gift card:** Prepaid / preloaded merchant instrument used for purchasing at specific merchants.
- **Gateway**: An enterprise that manages, on an out-sourced basis, various functions for a digital financial services provider. These functions may include transaction management, customer database management, and risk management. Processors may also do functions on behalf of payments systems, schemes, or switches.

- **Interchange Fees:** Fees paid by the acquirer to the issuer to compensate for transaction-related costs. VISA, MasterCard and other providers determine the interchange fee rates.
- **IMPS:** Immediate payment services is a product of NPCI which provided reals time payment to beneficiary on basis of mobile number up to 1 lac rupees.
- **Know Your Customer (KYC):** Set documents to establish business entities or person's credentials.
- **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.
- **Near Field Communication NFC:** A communication technology used within payments to transmit payment data from an NFC equipped mobile phone to a capable terminal.
- **NEFT:** National electronic fund transfer is a payment product of RBI for batch wise payments to beneficiary.
- **One Time Password (OTP):** An OTP or One Time Password is an added security measure that involves a two-step authentication for your online transactions. This time-bound OTP has become a very popular option for most financial transactions.
- **Phishing -** The fraudulent practice of sending emails purporting to be from reputable companies to induce/lure individuals to reveal personal information, such as passwords and credit card numbers.
- **Point of Sale Device Terminal, Acceptance Device, POS, mPOS**: Any device meant specifically for managing the receipt of electronic payments.
- **PCI-DSS:** The practices that enterprises do to protect end user data. "PCI-DSS" is a card industry standard for this.
- **P2P; Remote Cross-border Transfer of Value, Cross-Border Remittance:** Making and receiving payments to another person in another country.
- **Quick Response code (QR)-** A quick response (QR) code is a type of barcode that stores information and can be read by a digital device, such as a cell phone.

- **Reconciliation:** Reconciliation is an accounting process that uses two sets of records to ensure figures are correct and in agreement. It confirms whether the money leaving an account matches the amount that's been spent and ensures the two are balanced at the end of the recording period.
- **Recurring Payments:** Payments that we make periodically, and periodicity may be weekly, monthly, quarterly, half-yearly, yearly Example: Utility bill, insurance premiums.
- **Switch (National Financial Switch):** An entity which receives transactions from one provider and routes those transactions on to another provider. A switch may be owned or hired by a scheme or be hired by individual providers. A switch will connect to a settlement system for inter-participant settlement.
- **TAT:** Turn Around Time: Time committed for delivering a particular service (e.g. TAT for Settlement is T+2 day).
- **Unified Payment Interface (UPI):** UPI is a digital payment initiative by NPCI to boost digital payments in India and provide interoperability. Once customer registers for UPI with the bank, a unique virtual identifier is created and that is mapped to mobile phone to initiate the payment, UPI invokes this virtual identity of the beneficiary and transfers money in real-time. It works on single-click 2-factor authentication.
- **UTR:** UTR is Unique Transaction Reference number that is generated in IMPS, NEFT and RTGS system for uniquely identifying any transaction. The format of UTR is predefined and is generated by the bank initiating the transaction.
- **Wallet:** A wallet is an account for holding the funds and can be used for various purchases. A wallet can be virtual (e.g. mobile wallet such as Paytm, Phonepe or physical (prepaid cards).

****


भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

OFFICE OF RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA

Design by M Muralidhar, Anupam Sharma