





# **Nationwide Intensive Awareness Programme**

**An awareness initiative by Reserve Bank of India in collaboration with Regulated Entities**  
**(November 01, 2022 to November 30, 2022)**

# Table of Content



S. No.	Topic	Slide Number
1	Internal Grievance Redressal Mechanism	3-4
2	Alternate Grievance Redressal Mechanism	5-6
3	Safe Digital Banking Practices	7-11
4	Fraud Preventive Measures	12-14
5	Customer Protection Policy	15
6	Use of technology in Banking	16-17
7	Doorstep Banking Services for Senior Citizens and differently abled citizens	18-19
8	Banking Services available to MSMEs/Self Help Groups	20



## Unaware about what to do ?





# Internal Grievance Redressal Mechanism

## 1st line of Grievance Redressal

- ✓ Branch / ATM
- ✓ Instant Chat / Chat with Agent
- ✓ Speak with Us / Call Centre
- ✓ Connect via Email

## 2nd line of Grievance Redressal

- ✓ Write to Nodal Officer of the Bank
- ✓ Download the Grievance Form and send it to the address mentioned on it
- ✓ For branch related complaints, take up with Circle Nodal Officer

## 3rd line of Grievance Redressal

- ✓ Escalate to Principal Nodal Officer
- ✓ By clicking on the website to send an Email to PNO
- ✓ Download the Grievance Form and send it to the address mentioned on it

# Reserve Bank - Integrated Ombudsman Scheme



Single window for complaints against  
entities regulated by RBI

- Complaints not resolved within 30 days or not resolved satisfactorily by banks/NBFCs/system participants regulated by RBI, can be filed with the Ombudsman
- Lodge your complaint from anywhere, anytime
- Get acknowledgement and track status of your complaint on the Complaint Management System (CMS) portal
- For more information or to file a complaint, visit <https://cms.rbi.org.in>



**RBI Kehta Hai...  
Jaankaar Baniye,  
Satark Rahiye!**

For more details, visit <https://rbikehtahai.rbi.org.in/>  
For feedback, write to [rbikehtahai@rbi.org.in](mailto:rbikehtahai@rbi.org.in)



Issued in public interest by  
**भारतीय रिज़र्व बैंक**  
**RESERVE BANK OF INDIA**  
[www.rbi.org.in](http://www.rbi.org.in)



## Approach the RBI's Banking Ombudsman – the third umpire in banking

1. If the bank does not resolve your complaint to your satisfaction within a month, approach RBI's Banking Ombudsman
2. Banking Ombudsman Scheme is a cost-free and hassle-free way to resolve your banking complaints
3. Banking Ombudsman Scheme covers a range of deficiencies in banking services

# Alternate Grievance Redressal Mechanism Reserve Bank– Integrated Ombudsman Scheme, 2021

Steps to get resolution if you have a complaint against any bank or NBFC ?

**Banks / NBFCs**



No solution within one month or unsatisfactory resolution provided

**Office of RBI Ombudsman**



No solution within one month or unsatisfactory resolution provided

**Appellate Authority**



## Step 1

- Lodge a written complaint at Banks/NBFCs branches or website
- Wait for 30 days for Banks/NBFCs to resolve your complaint.
- If unsatisfied with the resolution given by Banks/NBFCs, go to step 2

### Escalation Matrix

**Branch Manager → Zonal Office → Head Office**

## Step 2

- Lodge complaint against Banks/NBFCs at Complaint Management System Portal at <https://cms.rbi.org.in>. or;
- Handwritten complaints addressed to Centralised Receipt & Processing Centre, Reserve Bank of India
- For complaint related queries, call toll free number 14448

## Step 3

- The customer can file an appeal before appellate authority within 30 days. If not happy with the solution provided by the Ombudsmen
- The appellate authority is the Deputy Governor of the Reserve Bank of India (RBI)



## Safe Digital Banking

- Don't share your passwords, PIN, OTP, CVV, etc. with anyone online or through phone
- Never click on suspicious links that you receive via SMS, email or social media platforms







# Safe Digital Banking Practices



## **Dos for Safe Banking Practices**

- ✓ Always go to official websites of banks/service provider and use websites which are secured for e.g., https:// - where 's' stands for secured website
- ✓ Log out of all payment/financial apps from your mobile/laptop/PC if they are facing technical glitches or while downloading apps
- ✓ Check the spellings of websites/URLs being accessed to avoid fraudulent, fake and look-alike websites similar to banks or e-commerce platforms
- ✓ Check spellings and headers of emails received to ensure that the emails are from authentic addresses
- ✓ Be careful while clicking on shortened URLs / google forms received through SMS/ Whatsapp/ email, etc.
- ✓ Block/Unsubscribe/ report as spam mails providing links to banks/ecommerce/search engine websites
- ✓ Be careful while buying/selling products online. To receive money through UPI there is no need to enter PIN/password
- ✓ Contact your mobile operator immediately if there is no mobile network in your phone for considerable period of time in a regular environment
- ✓ Check SMS/emails regularly to ensure that no OTP is generated without your prior knowledge
- ✓ Before transacting with any company, verify if they are registered and licensed entity
- ✓ Turn on two factor authentication wherever such facility is available
- ✓ While using ATM, cover keypad with your other hand while entering PIN
- ✓ If cash is not dispensed, press 'Cancel' on ATM and leave only after the home screen appears
- ✓ Note that customer care numbers are never in the form of mobile numbers
- ✓ While depositing cash in CDM, ensure that the cash is accepted by the machine before leaving the premises
- ✓ Always check whether any extra device is attached near card insertion slot or keypad of ATM machine

# Safe Digital Banking Practices



## Don'ts for Safe Banking Practices

- ❖ Don't trust strangers and take help from them at ATMs as the credentials may get stolen
- ❖ Don't share details of SIM card and mobile number or write PIN on ATM card or save details on websites/devices/public laptops/desktops
- ❖ Don't get trapped by offers from persons posing as call centre agents from banks, insurance, government etc. and don't get pressurized/tricked into sharing username, password, card details/PIN/CVV/OTP, date of birth, Aadhaar number, names of family members, etc.
- ❖ Don't search for contact details of service providers from search engines, SMS, social media, emails, etc.
- ❖ Don't click on unknown/unverified links and don't download apps from unverified sources on advice of unknown people
- ❖ Don't permit your bank accounts/ATM cards to be used by others, for a commission or otherwise, which may lead to police investigation due to misuse of bank account for routing money
- ❖ Don't respond to calls/emails/SMS seeking your KYC details/account details/ATM card details/PIN/CVV/OTP details
- ❖ Don't trust unbelievable lottery offers and share secure credentials in response to such emails/calls
- ❖ Don't respond to messages claiming that huge amount is lying with RBI and some amount needs to be transferred to get it released
- ❖ Don't get defrauded by paying upfront loan processing fee in cash
- ❖ Don't respond to messages offering/promising prize money, government aid and KYC updation to receive money/recharge mobile balance/to get a job
- ❖ Don't make payments or enter secure credentials against online offers of loans at low interest rate/ secure instant loan
- ❖ Don't use screen sharing apps on the same device where financial apps are being used
- ❖ Don't scan QR codes using unknown payment apps which may be used for transferring money out after keying in the UPI PIN
- ❖ Don't use public charging points or unsecured Wi-Fi as they can be used to transfer malware and take control of data from the phone

# Electronic Banking



## Dos

- Always type your bank's URL using only verified and trusted browsers and HTTPS secured websites for payments (S stands for Secure). Look for secure sign (lock) in the URL window (image)
- Make your passwords difficult to guess, by using alphanumeric and special characters (#.", @. \$ etc.)
- Ensure that you change your password frequently
- Always keep your payment transaction Apps (banks, non-banks, Wallets etc) updated with the latest version
- Link your mobile number and email ID with your bank account and opt for SMS/e-mail alert service
- In case of any unusual/unauthorized transaction, inform the bank immediately

## Don'ts

- Never access your bank's website through online search.
- Never store login credentials on phone, also don't enter/store credentials on untrusted portals/service providers
- Avoid transacting through public devices, cyber cafes and on unsecured/open networks like public/free WiFis
- Never share your mobile banking PIN or Internet banking ID, password and OTP with anyone (including bank staff)

# Unified Payment Interface (UPI)



## Dos

- Keep UPI App updated
- Always review the merchant/person's collect request before accepting it
- Recheck and re-confirm the amount and beneficiary before effecting the transfer

## Don'ts

- Never share your PIN with anyone
- Refrain from transferring money without verifying/reconfirming the recipient first

# Consumer Awareness - Cyber Threats and Frauds



Fraudsters attempt to get confidential details like user id, login / transaction password, OTP (one time password), debit / credit card details such as PIN, CVV, expiry date and other personal information. Some of the typical modus operandi being used by fraudsters are –



**Vishing** - phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers in order to lure customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.



**Phishing** - 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.



**Remote Access** - by luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.



Misuse the 'collect request' feature of UPI by sending fake payment requests with messages like 'Enter your UPI PIN' to receive money.



Fake numbers of banks / e-wallet providers on webpages / social media and displayed by search engines, etc.

# Steps to be taken if a fraud occurs



Contact your bank/NBFC and block your account/card immediately and submit a written complaint



Lodge a complaint/FIR with Indian Cyber Crime Coordination Centre or call cybercrime helpline number 1930



Contact your branch for blocking funds in beneficiary account(s)



Escalate matter to RBI Ombudsman if the bank/NBFC fails to resolve your complaint.

# Don't let anyone score against you

Never share your Password, PIN, OTP, CVV, UPI-PIN, etc., with anyone



**Rasika Raju**  
Indian Badminton Player and  
RBI Employee

**Poorvisha S. Ram**  
Indian Badminton Player and  
RBI Employee



## Digital/Online Fraud Prevention

- Register your mobile number and email with your bank to get instant alerts
- Never store important banking data in mobile, email or purse
- Use only verified, secure and trusted websites for online banking
- Avoid banking through public, open or free networks
- Change your online banking password and PIN regularly
- Block your ATM Card, Debit Card, Credit Card, Prepaid Card immediately if it is lost or stolen



# Customer Protection Policy



## **Strengthening of systems and procedures- The systems and procedures in banks to make customers feel safe about carrying out electronic banking transactions**

- Robust and dynamic fraud detection and prevention mechanism;
- Mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;
- Appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom;
- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud
- Transparent, non-discriminatory and stipulated mechanism to compensate the customers for unauthorized electronic banking transactions

# Use of Technology in Banking

- **Digital Banking is 'Convenient' and 'Safe' too. Transact anytime, anywhere.**
- Banking on your fingertips, from the comfort of your home
- Saves time through quick and safe payments
- Multiple digital payment options for various transactions
- NEFT, IMPS, UPI and BBPS available 24x7



## Do not have a smartphone or access to the Internet?

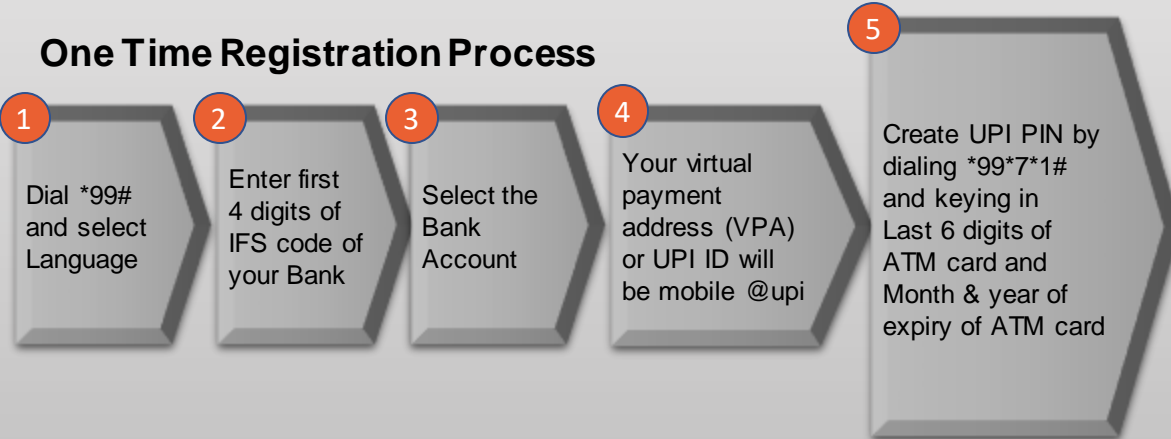
### Go Digital Using \*99#

A platform that allows transfer of money between two bank accounts using a feature phone/smart phone without internet connection by dialing USSD code (\*99#)



- Using your UPI Pin, you can transfer funds seamlessly to any beneficiary by just knowing the beneficiary's virtual address.
- If the beneficiary doesn't have a virtual address, the option of transferring funds to the beneficiary through IFSC and Account number or Aadhaar number linked to bank account or mobile number is also available.
- With "998, one can transfer funds to a recipient registered on UPI and #998

### One Time Registration Process



## Do you have a smartphone with access to the Internet?

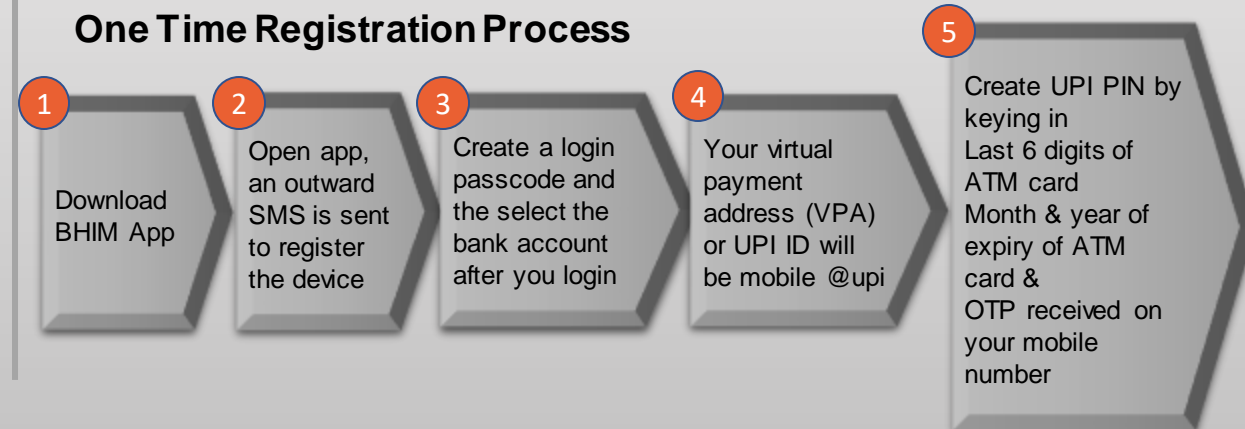
### Go Digital Using on the Unified Payments Interface (UPI) platform

A platform that allows transfer of money between two bank accounts using a mobile phone which has access to the internet



- Using your UPI PIN, you can transfer funds seamlessly to any beneficiary by just knowing the beneficiary's virtual address. If the beneficiary doesn't have a virtual address, the option of transferring funds to the beneficiary through IFSC and Account number is also available.

### One Time Registration Process



# Doorstep Banking Services for Senior Citizens and differently abled citizens

## **RBI has asked banks to make banking convenient for senior citizens**

- If you are above 70 years, you can receive certain basic banking facilities at your home
- Banks automatically convert fully KYC compliant account into 'Senior Citizen Account' on the basis of date of birth available in banks' records
- Banks provide dedicated counters in their branches where senior citizens get priority for their banking needs

## **Ease of banking for senior citizens**

**RBI has asked banks to make banking convenient for senior citizens**



**Umesh Yadav**  
Indian Cricketer and  
RBI Employee

# Banking Services for Differently abled citizens



- Banks ensure that all the banking facilities such as cheque book facility including third party cheques, ATM facility, Net banking facility, locker facility, retail loans, credit cards etc., are invariably offered to the visually challenged without any discrimination
- At least one talking ATM with **Braille keypad** is generally available in each locality for catering to the needs of visually impaired persons



- Banks ensure that **all existing ATMs / future ATMs with ramps** so that wheelchair users / persons with disabilities can easily access them and arrangements are made in such a way that the height of the ATM does not create an impediment in its use by a wheelchair user.
- **Banks also take appropriate steps by providing ramps at the entrance of the bank branches** so that the persons with disabilities / wheelchair users can enter the bank branches and conduct business without much difficulty.



# Banking Services available to MSMEs/Self Help Groups



## KYC for SHG savings accounts:

- KYC verification of all the members of the SHG need not be done while opening the savings bank account of the SHG.
- The KYC verification of all the office-bearers would suffice.
- However, resolution of SHG indicating the name of office-bearers authorized to open the account on behalf of the SHG is required to be submitted.

## Margin and security norms

- No collateral security to be obtained from SHGS for availing loans
- Loan amount of more than four times of the corpus is possible if SHGS are functioning successfully for many years.  
The SHGS have repaid past loans on time.  
The SHGS have used the credit facility responsibly.

## Voluntary Savings

- Voluntary savings can be reckoned in two ways:
  - ❖ Not forming a part of the group corpus
  - ❖ As a part of the group corpus and utilized for intra-group lending
- Voluntary savings will also be reckoned for assessing the quantum of loan to the group from bank which might benefit your SHG as the SHG might get a larger quantum of loan from the bank. The members of the SHG will jointly decide whether the voluntary savings by members of the group are eligible for proportionate share in the interest Income or dividend from the group.

