CHAPTER - 3

Digital Financial Literacy

1. Retail Remittances

NEFT, RTGS and IMPS are the most popular remittance channels offered by banks to transfer money. They can be availed at the bank branch or through online channels like Internet banking, mobile banking etc. offered by your bank

1. खुदरा लेन-देन

एनईएफटी, आरटीजीएस, और आईएमपीएस बैंकों द्वारा धन हस्तांतरित करने के लिए सबसे लोकप्रिय लेन-देन के माध्यम हैं। इन सुविधाओं का लाभ बैंक शाखाओं अथवा बैंक द्वारा उपलब्ध ऑनलाइन माध्यमों, जैसे: इंटरनेट बैंकिंग, मोबाइल बैंकिंग आदि के जरिये भी किया जा सकता है।

Here's a graphic that explains the three channels:

Features	NEFT	RTGS	IMPS
Time taken to transfer	Within an hour	Immediately	Immediately
Working hours for customer transactions	24/7- Round the clock even on weekends and bank holidays	24/7- Round the clock even on weekends and bank holidays	24/7- Round the clock even on weekends and bank holidays
Minimum amount required	No minimum amount	₹2 Lakhs	No minimum amount
Maximum amount that can be transferred	Any Amount	Any Amount	₹5 lakhs

2. Unified Payments Interface

Unified Payments Interface or UPI is a platform that allows transfer of money between two bank accounts using a smartphone which has access to the internet. You can use the BHIM app or any of the banks' app or any third-party app for facilitating UPI transactions.

2. यूनीफाइड पेमेंट्स इंटरफेस

यूनीफाइड पेमेंट्स इंटरफेस या यूपीआई एक ऐसा प्लेटफॉर्म है जो इंटरनेट की सुविधा वाले स्मार्टफोन का उपयोग करके दो बैंक-खातों के बीच धन हस्तांतरण की अनुमति देता है। यूपीआई लेनदेन की सुविधा के लिए आप भीम ऐप या बैंकों के किसी भी ऐप या किसी भी अन्य पक्ष के ऐप का उपयोग कर सकते हैं।

How does it work

Requirements:

You need a bank account, a mobile number linked to that bank account, and a smartphone with internet connection. To facilitate feature phone users to avail benefits of UPI, UPI123Pay was

launched with 4 options, viz., App based functionality, Missed Call, IVR, Proximity Sound based payments. Debit card linked to the account is required one time for setting-up UPI on mobile phone. UPI can also be linked to RuPay Credit Cards.

यह कैसे काम करता है
आवश्यकताः

आपको एक बैंक खाता, उस बैंक खाते से जुड़ा एक मोबाइल नंबर और इंटरनेट की सुविधा वाले एक स्मार्टफोन की आवश्यकता होगी। फीचर फोन उपयोगकर्ताओं के लिए यूपीआई की सुविधा हेतु, UPI123 पे को 4 विकल्पों के साथ लॉन्च किया गया था, जो इस प्रकार हैं: ऐप आधारित कार्यक्षमता, मिस्ड कॉल, आईवीआर, प्रॉक्सिमिटी साउंड आधारित भुगतान। मोबाइल फोन पर यूपीआई सेटअप करने के लिए खाते से जुड़े डेबिट कार्ड की एक बार आवश्यकता होती है। यूपीआई को रुपे क्रेडिट कार्ड से भी लिंक किया जा सकता है।

How to activate UPI

- Download the App on your smartphone and link bank account and create a UPI PIN by following the instructions given in the App
- Use of UPI: Using your UPI Pin, you can transfer funds seamlessly to any beneficiary by just knowing the beneficiary's virtual address or UPI number.
- If the beneficiary doesn't have a virtual address or UPI number, the option of transferring funds to the beneficiary through IFSC and bank account is also available.

यूपीआई को कैसे एक्टिवेट करें

- अपने स्मार्टफोन पर ऐप डाउनलोड करें और बैंक खाते को लिंक करें और ऐप में दिए गए निर्देशों का पालन करके अपना यूपीआई पिन बनाएं।
- यूपीआई का उपयोगः अपने यूपीआई पिन का उपयोग करके, आप लाभार्थी के वर्चुअल पते या यूपीआई नंबर के माध्यम से धन हस्तांतरित कर सकते हैं।
- यदि लाभार्थी के पास वर्चुअल पता या यूपीआई नंबर नहीं है, तो आईएफएससी और बैंक खाते के माध्यम से भी लाभार्थी को धन हस्तांतरित करने का विकल्प उपलब्ध है।

3. Dos and Don'ts for Electronic Banking Transactions
3. इलेक्ट्रॉनिक बैंकिंग लेन-देन में क्या करें और क्या न करें

Online and Mobile Banking
ऑनलाइन और मोबाइल बैंकिंग

✔ **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, nonbanks, 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/unauthorised transaction, inform the bank immediately.

✔ **करें**

- भुगतान के लिए हमेशा केवल सत्यापित और विश्वसनीय ब्राउज़रों और HTTPS सुरक्षित वेबसाइटों का उपयोग करते हुए अपने बैंक का URL लिखें (S का अर्थ सुरक्षित है)। URL विंडो (इमेज) में सुरक्षित चिह्न (लॉक) देखें
- अक्षरों, संख्याओं (अल्फान्यूमेरिक) और विशेष वर्णों (#, *, @, $ आदि) का उपयोग करके अपने पासवर्ड को सुदृढ़ बनाएं।
- सुनिश्चित करें कि आप अपना पासवर्ड समय-समय पर बदलते हैं
- हमेशा अपने भुगतान लेनदेन ऐप्स (बैंक, गैर-बैंक, वॉलेट आदि) को नवीनतम संस्करण के साथ अपडेट रखें
- अपने मोबाइल नंबर और ईमेल आईडी को अपने बैंक खाते से लिंक करें और एसएमएस/ई-मेल अलर्ट सेवा का विकल्प चुनें
- किसी भी असामान्य/अनधिकृत लेनदेन के मामले में, तुरंत बैंक को सूचित करें।

✘ **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).

✘ न करें

- कभी भी ऑनलाइन खोज के माध्यम से अपने बैंक की वेबसाइट को एक्सेस न करें।
- कभी भी फोन पर सर्च क्रेडेंशियल स्टोर न करें, अविश्वसनीय पोर्टल/सेवा प्रदाताओं पर क्रेडेंशियल दर्ज/स्टोर न करें।
- सार्वजनिक उपकरणों, साइबर कैफे और सार्वजनिक/मुफ़्त वाईफाई जैसे असुरक्षित/खुले नेटवर्क के माध्यम से लेनदेन करने से बचें।
- कभी भी अपना मोबाइल बैंकिंग पिन या इंटरनेट बैंकिंग आईडी, पासवर्ड और ओटीपी किसी के साथ (बैंक स्टाफ सहित) साझा न करें।

4. Dos and Don'ts for ATM Transactions

4. एटीएम लेन-देन में क्या करें और क्या न करें

✔ Dos

- Ensure that you use only EMV Chip and PIN based Debit Card instead of card with a magnetic strip (Approach your bank for replacing the magnetic strip card).
- Ensure that there are no unauthorized cameras or other skimming devices near ATMs when you key-in your PIN or swipe your cards.
- Make sure no one sees the PIN when it is being entered at the ATM. It is a good practice to cover the keypad with one hand and use the other hand to key-in your PIN.
- Remember to count and check the notes dispensed.
- Remember to collect your card after the transaction is over
- Register your phone number with card issuing bank to get alerts on ATM transactions.
- Contact your bank immediately to block the card if it gets lost or stolen or if you feel it has been compromised

✔करें

- सुनिश्चित करें कि आप चुंबकीय पट्टी वाले कार्ड की बजाय केवल ईएमवी चिप और पिन आधारित डेबिट कार्ड का उपयोग करें (चुंबकीय पट्टी वाले कार्ड को बदलने के लिए अपने बैंक से संपर्क करें)।
- सुनिश्चित करें कि जब आप अपना पिन दर्ज करते हैं या अपने कार्ड स्वाइप करते हैं तो एटीएम के पास कोई अनधिकृत कैमरा या अन्य स्किमिंग डिवाइस नहीं है।
- सुनिश्चित करें कि एटीएम में पिन दर्ज करते समय कोई भी इसे नहीं देख रहा हो। एक हाथ से कीपैड को कवर करना और अपने पिन को दर्ज करने के लिए दूसरे हाथ का उपयोग करना एक अच्छी आदत मानी जाती है।
- प्राप्त नोटों को गिनें और जाँचें।
- लेन-देन समाप्त होने के बाद अपना कार्ड वापस अवश्य लें।
- एटीएम लेनदेन पर अलर्ट प्राप्त करने के लिए कार्ड जारी करने वाले बैंक के साथ अपना फोन नंबर पंजीकृत करें।
- कार्ड खो जाने या चोरी होने अथवा यदि आपको ऐसा लगता है कि इससे छेड़छाड़ की गई है, तो उसे ब्लॉक करने के लिए तुरंत अपने बैंक से संपर्क करे।

✘ **Don'ts**

- Do not share your ATM card details (card no., expiry date and CVV etc.) and PIN with anyone.
- Never leave the Card in the ATM.
- Never share your OTP with anyone.
- Never write vour PIN on the Card.

✘ **न करें**

- अपने एटीएम कार्ड का विवरण (कार्ड नंबर, समाप्ति तिथि और सीवीवी आदि) और पिन किसी के साथ साझा न करें।
- कभी भी एटीएम मशीन में कार्ड न छोड़ें।
- कभी भी अपना ओटीपी किसी के साथ साझा न करें।
- कार्ड पर कभी भी अपना पिन न लिखें।

5. Customer Liability for Fraudulent (Digital) Transactions

Notify your bank

- Irrespective of whose fault it is, notify your bank immediately if you encounter a fraudulent or unauthorized electronic banking transaction in your account/ Card
- The longer you take to notify the bank, higher is the loss to you or your bank

5. धोखाधड़ीपूर्ण लेन-देन (डिजिटल) के लिए ग्राहक की देयता

अपने बैंक को सूचित करें

- चाहे किसी की भी गलती हो, यदि आप अपने खाते / कार्ड में धोखाधड़ी या अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन का सामना करते हैं, तो तुरंत अपने बैंक को सूचित करें।
- बैंक को सूचित करने में आपको जितना अधिक समय लगेगा, आपको या आपके बैंक को उतना ही अधिक नुकसान होगा।

Bank's responsibility

If the fraudulent transactions continue even after you have informed the bank, the bank will have to bear the loss

- Your bank has to provide an acknowledgement for the complaint when you notify/inform the bank
- The bank must resolve your complaint within 90 days
- Bank shall credit the amount involved to the customer's account within 10 working days from the date of such notification by customer

बैंक की जिम्मेदारी

अगर आपके द्वारा बैंक को सूचित करने के बाद भी धोखाधड़ी वाले लेनदेन जारी रहते हैं, तो बैंक को नुकसान उठाना पड़ेगा।

- जब आप बैंक को सूचित करते हैं तो आपके बैंक द्वारा शिकायत के लिए एक पावती प्रदान करनी होती है।
- बैंक को 90 दिनों के भीतर आपकी शिकायत का समाधान करना होगा।
- बैंक संबंधित ग्राहक द्वारा दी गयी सूचना की तारीख से 10 कार्य दिवसों के भीतर ग्राहक के खाते में संबंधित राशि जमा करेगा

Limited Liability

- If loss is due to negligence of the customer (sharing password etc.) then customer will bear the loss till the bank is informed.
- If there is no negligence of the customer, and the customer informs the bank immediately (within 3 working days of the unauthorized transaction), there is no liability of the customer.
- In case of negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer), there is no liability of the customer.
- In case of third party breach where the deficiency lies in the system and not with the customer or the bank and the customer informs the bank immediately (within 3 working days of the unauthorized transaction), there is no liability of the customer.

सीमित देयता

- यदि नुकसान ग्राहक की लापरवाही (पासवर्ड साझा करना, आदि) के कारण होता है तो बैंक को सूचित किए जाने तक ग्राहक को नुकसान उठाना होगा।
- यदि ग्राहक की कोई लापरवाही नहीं है, और ग्राहक तुरंत बैंक को सूचित करता है (अनधिकृत लेनदेन के 3 कार्य दिवसों के भीतर), तो ग्राहक की कोई देयता नहीं होगी।
- बैंक की ओर से लापरवाही/कमी के मामले में (ग्राहक द्वारा लेन-देन की सूचना दी गयी हो या नहीं), ग्राहक की कोई देयता नहीं होगी।

किसी तीसरे पक्ष द्वारा उल्लंघन के मामले में जहां सिस्टम में कोई कमी है और वह ग्राहक या बैंक से संबंधित नहीं हैं, और ग्राहक तुरंत बैंक को इस बारे में सूचित करता है (अनधिकृत लेनदेन के 3 कार्य दिवसों के भीतर), तो ग्राहक की कोई देयता नहीं होगी।