ओरियन्टल बैंक ऑफ़ कॉमर्स
Oriental Bank of Commerce

Annexure-I

ओरियन्टल बैंक ऑफ़ कॉमर्स
Oriental Bank of Commerce

FRAUD REPORTING FORM
(For Electronic Channel Transactions only)

**Mandatory Fields*

Account Number*								Branch					
Account/ Customer's Name*													
Tick applicable box*	Debit Card		I-Bank		M-Bank		AEPS		UPI		USSD		Others : ______
ATM/ Debit Card No.									(Mandatory for card related frauds only)				
You came to know about the fraudulent transaction through	SMS		EMAIL		Call from Bank		Bank Statement		Passbook		Others (Please specify)		
Regd. Mobile No.*							E-Mail ID						
Any Other Contact No													
Customer complaint statement in brief													

I wish to report the following transaction which have been done fraudulently through the electronic channel for Debit to my above mentioned account through the said channel(s)

S. No.	Transaction Date (DD/MM/YYYY)* & Time	Transaction/ Reference no.	Amount Debited to the Account (in ₹)*

Please list your unauthorized transaction below. Do not include any fees incurred.

Please provide the information on the below mentioned questions, as applicable:							
1.	At the time of the fraudulent transaction(s), your Debit Card was:						
	In my possession		**Lost/ Stolen**		**In my possession**		
2.	Detail of last transaction done by you through your debit card						
3.	If lost or stolen, when did you discover it was missing?						
4.	**Have you ever given your card or card number and PIN/OTP to someone else to complete a transaction for you:**						
	Yes		No		If Yes, then please provide	**Name** / **Relationship** / **Address**	
5.	Detail of FIR (If not filed please provide the reason)						
6.	Spoof/ Fraud Website Address						
7.	Fraudster Mobile no/Phone No (If available):						

I give my consent to the Bank to release/share any information regarding my account to any local, state, and/or law enforcement agency to be used in the investigation and prosecution of any person(s), who may be responsible for fraud involving my account.

Place:

Date:

Account holder/ Card holder Signature

To be filled by Branch						
Branch Sol ID:	Branch Name:					
We have physically verified the Debit Card under dispute and confirm the same is in the possession of customer (Tick as applicable)	Yes		No		Not applicable	
We hereby confirm the above mentioned details and attach the following documents:- 1. Copy of Aadhaar Card or PAN of Customer (Mandatory) 2. Copy of FIR by customer						
Remarks by Branch office						
Name & Designation: Date:	Signature of Branch Manager/ Hall In-Charge Branch:					

In case of any queries, please contact the Call Center at numbers **1800-180-1235, 1800-102-1235 OR 0120-2580001 or** contact your Branch.

Annexure II

SECTION OF POLICY FOR PUBLIC DISCLOSURE

"CUSTOMER PROTECTION/ COMPENSATION POLICY-UNAUTHORISED/ FRAUDULENT ELECTRONIC TRANSACTIONS"

I. INTRODUCTION

Reserve Bank of India vide Circular No. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/ 2017-18 dated 06th July'2017 have issued guidelines on "Customer Protection- Limiting Liability of customers in unauthorized Electronic Banking Transactions."

The guidelines bring out the regulation for determining the customer liability in case of the unauthorized transactions resulting in debits to their accounts/ cards through electronic medium along with the compensation by Banks to customer for the unauthorized transactions.

The aforesaid guideline by Reserve Bank of India supersedes some of the instructions in respect of fraudulent/ unauthorized transaction along with related provisions for security, risk mitigation, customer liability, reporting etc. as contained in Master Circular DBR No. FSD.BC. 18/24.01.009/2015-16 dated 01st July'2015 on "Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card operations of Banks and Credit Card issuing NBFCs."

II. OBJECTIVE

The objective of this policy is to communicate the following in a fair and transparent manner for the bank's electronic channel (e-channel) transactions viz. Debit Cards, Pre-Paid Cards, ATM, Internet Banking, Mobile Banking, other mobile based application such as UPI, BHIM, Aadhaar enabled payments:

a. Creating awareness to the customer on the risks involved and their responsibilities when transacting through e-channel
b. Customer liability in case of unauthorized e-channel transaction
c. Customer compensation and its defined time lines for its eligibility

III. SCOPE OF THE POLICY & APPLICABILITY

The policy covers the aspects of electronic channels with respect to the redressal of the customer grievances for unauthorized/ fraudulent transactions due to:

a) Contributory fraud/ negligence/ deficiency on part of the Bank
b) In case of customer negligence by sharing of the payment credentials such as Card credentials, OTP, PIN, Login credentials, passwords etc.
c) Due to third party breach of system where the deficiency lies neither with the Bank nor due to customer's negligence and/or contributory negligence.
d) Any other electronic modes which is currently being used or adopted in future.

This policy determines the liability of the Bank and/ or Customer for such unauthorized/ fraudulent transaction for determining the extant of the compensation under the stated policy.

Categories of Customer for applicability of Policy:

a) This policy is **applicable** to entities that hold relationship with the bank viz:
    i. Individual and non-individual customers who hold savings and current account
    ii. Individual and non-individual entities who hold bank issued Debit card or Pre-paid cards
    iii. Individual and non-individual entities who use bank's e-channels
b) This policy is **not applicable** to:
    i. Non-Customer that use Bank's infrastructure e.g. ATMs & UPI
    ii. Entities that are part of the ecosystem such as Intermediaries, Agencies, Banking Correspondents, Franchises, payment gateways, service partners, Vendors, Merchants etc.

Exclusion of Transactions:

a) This policy shall not be applicable on the disputed transactions on electronic channels related to Failed ATM transactions, Failed POS transactions and Failed ecommerce transactions done using Debit/Credit card or Internet Banking or Mobile Banking (Allied applications like UPI, BHIM, Aadhaar Pay) which shall be handled through Chargeback mechanism for such failed transactions.

b) This policy also excludes e-channel transactions effected on account of error by a customer either to incorrect payee or amount, transactions done under duress, opportunity loss claims, loss of reputation or incidental costs or collateral damage.

IV. POLICY FRAMEWORK

The framework of the policy covers the aspects of compensation for the financial loss arising out of Unauthorized/ fraudulent electronic transactions and as such the commitments under the Policy are without prejudice to any right the bank will have in defending its position before any forum duly constituted to adjudicate banker-customer disputes, if required.

A. ELECTRONIC TRANSACTION TYPES

The electronic transactions can be broadly classified based on the customer channel access requiring physical presence at the point of transaction or undertaken remotely, which are as under:

- **Remote/ Online payment transactions**

  The remote/ online payment transactions are those payment types which doesn't requires the physical presence of the payment instrument at the point of transactions.

  Eg: Payment transaction initiated directly or indirectly routed from host site and payment done through Mobile Banking, Internet Banking, UPI/ BHIM etc. for NEFT/ RTGS/ IMPS/ Transfer transactions/Bill Payments/Ticket Booking and also transactions undertaken using Card (Credit/ Debit/ Prepaid) on eCommerce platform (Card Not Present-CNP), link based payments etc.

- **Face-to-Face/ Proximity payment transactions**

  The payment transactions requiring physical presence of the payment instruments at the point of transactions can be classified as Face-to-Face/ Proximity payment transactions.

  Eg: Payment transactions initiated through Card at ATMs or at Business Correspondent (BC/ POT), Card at POS including swipe/ dip of card, tap & go payments, NFC (Near Field Communication) based payments, transaction on BC/POT/ Merchants using Aadhaar details etc. The usage of the mobile devices for making proximity payments through NFC, QR based payments etc.

B. DEFINITIONS

i. Unauthorized transactions on Electronic channels

Unauthorized/ fraudulent transactions on electronic channels are such transactions which have not been authorized by the customer through specified process of authentication on respective channels.

However, these transactions have been effected in the customer Card/ account by way of contributory negligence on the part of customer by sharing payment credentials, negligence/ deficiency/ contributory fraud ascertained on the part of Bank or due to a third party breach wherein the deficiency lies neither with the Bank or the customer.

ii. Electronic channels

Electronic channels are part of the payment system which provides the customer report access to Banking facilities as well as facilitates to undertake the payment transaction upon self without requiring any physical presence by payment system participants such as Bank or its agents to a transaction. The electronic channels include payment instruments & types as briefed under section V sub section (A).

iii. Working Days

Working day or Business day shall be considered as the days on which the parent branch of the customer is open for undertaking business activities as per respective jurisdiction. The counting of working day shall exclude the date of receiving the communication and subsequent non-working days as declared by Central/State Governments/Union Territory under the Negotiable Instruments (NI) Act for the unauthorized transaction.

iv. Payment credentials

Payment credentials refer to the details required to undertake a transaction using Card or Internet Banking or mobile application. The payment credentials are personal information which must be protected by the customer and shall always undertake reasonable security to not to share/ disclose such credentials with any other party. The compromise of the payment credentials may lead to unauthorized or fraudulent transactions. These credentials includes Card number, Expiry date, CVV, PIN, OTP (One Time Password),

Login ID/ User name, Password (Login/ Transaction), M-PIN, application login PIN/ Password, secret question and its corresponding answers, any method of resetting such channels password/ PIN etc.

Further, with the increase in the usage of the Smartphone devices as payment instrument, it is critical that the SIM card related credentials i.e. SIM number of the registered mobile number with the Bank shall not be disclosed by the customer to any other party, which may lead to compromise of customer SIM Card in turn abetting in negligence or otherwise, unauthorized/ fraudulent transactions in their Card/ accounts.

C. BRIEF ON SAFETY & SECURITY MEASURES

Bank have implemented robust system for safeguarding the access to Card and online/ electronic payment instruments by maintaining Payment Card Industry Data Security Standards (PCIDSS) and Information Security Standards (ISO 27001: 2013).

The security standard varies from channel to channel while ensuring a balance between security and customer convenience. The transactions are authorized using 2 Factor of Authentication (2FA) in all the channels, which is briefed as under:

- **Debit Cards**: In the proximity based transaction using Debit cards at ATM or POS, the transactions are being authorized using input of PIN by the customer. The customer shall at all times safeguard the physical card and PIN. However, for e-commerce transaction (domestic), the customer is required to input Card credentials i.e. Card number, expiry date & CVV and then input the dynamic OTP (One Time Password) received on registered mobile number for authorizing the transaction, which is valid for one transaction only within a time limit of 5 Minutes for RuPay & 10 Minutes for Visa Cards. However bank has allowed international e-commerce transactions without second factor authentication(i.e. OTP) from 50 sites under ECI-7 category for VISA Debit cards

  Also, the customer Card credentials to an extent of Card number (Masked) and expiry date is stored by payment gateway or in host websites (for registered users), wherein the customers are required to input the CVV number and OTP for authorizing the transaction.

Bank has re-carded active Magstripe cards with more secure EMV chip based cards in line with RBI directives.

Further, for handover of the cards at branches, an authorization code is sent to customer registered mobile number for handover of the Debit Card (Personalized) which is entered in Card Management System (IDEAS) to activate the Card for usage as well as acts as a confirmation for customer receipt.

i. **Internet Banking**: The Retail Internet Banking application requires user to input the User ID and login password for user access and with second factor of authentication requiring customer to input transaction password and OTP for validating the transaction *(except for transaction in self linked accounts where only transaction password is required to authenticate the transaction).*

The additional authentication process in Retail Internet Banking requires prior addition of the beneficiaries with cooling period of 24 hours along with intimation to Registered Mobile number and E-Mail ID of the customer for beneficiary addition. The beneficiary and transaction type wise limits are also required to be pre-set by the customer before undertaking the financial transactions.

As a security measures for I-Banking, Bank provides user with the 'Image & Phrase' combination as a preemptive measure to identify genuine website to avoid phishing attack along with 3 source internet IP address IP check wherein every 4th new source IP requires authentication through dynamic OTP sent on registered mobile number for login.

However, in case of Govt. taxes/ payments and transfer to self linked accounts, validation is done through transaction password only i.e. no OTP is required for validation.

User ID, Login Password and Transaction Password expires if not used for 180 days, in case of expired user ID customer can themselves reset using Card credentials.

In Corporate Internet Banking pre-authorized shopping mall(e-commerce) transactions are only allowed where a Maker/Initiator can initiate a shopping mall/e-commerce transactions after taking approval from the Approver which is valid for 24 Hours with the given limit.

iii. **Mobile Applications:** The mobile applications such as Mobile Banking, UPI/ BHIM, BharatQR etc. authorizes the customer login using registered mobile number for user identification or by way of input of Customer ID or Mobile number or User ID, as the case may be, with the login password/ Application PIN to login to the application.

Also, mobile based application for Mobile Banking, UPI/BHIM and Bharat QR, facilitates remote customer on boarding by way of primary identifier as Mobile number combined with Card credentials or A-PIN/ Password to create the customer login.

iv. **Adaptive Authentication on Digital Channels**: Bank has also included additional layer of adaptive authentication based security wherein based on customer set challenge questions, risk engine randomly on the basis of risk threshold set-up the authentication with challenge question to ensure authenticity of the user in such high risk transactions scenarios. The adaptive authentication is an overlay security feature which has been implemented on both Internet & Mobile Banking platform.

D. CONTINUOUS AWARENESS

Bank send regular SMS to the customer to not to disclose payment credentials or payment system related information to any other party. The awareness drive through SMS, E-Mails, workshops etc. shall continued to be undertaken by the Bank.

E. OBLIGATION AND RIGHTS OF THE CUSTOMER

a) Customer is entitled to
   i. SMS alerts on valid registered mobile number for all financial electronic debit and credit transactions. In case the customer doesn't registers/ update their mobile number or subscribe to the SMS alerts or doesn't pay the standard charges for the SMS alerts, in such cases, then Bank shall be constrained or unable to inform or update the customer with the account activity, which in turn shall jeopardize banks capability to protect the customer under the ambit of this policy.
   ii. Email alerts where valid email Id is registered for alerts with the Bank
   iii. Register complaint through multiple modes – as specified in section F

iv. Customer compensation policy (E-channels) as per Annexure II online via Bank's Corporate Website.

v. Receive compensation in line with this policy document where applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and with customer liability being limited as specified in Section G & H.

b) Customer is bound by following obligations with respect to banking activities:

i. Customer shall mandatorily register valid mobile number with the Bank. Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer liability.

ii. Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint/ FIR as applicable and provide copy of the same to the Bank.

iii. Customer must not share sensitive information (such as Debit/Credit Card details & PIN, CVV, Internet Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff

iv. Customer should co-operate with the Bank's investigating authorities and provide all assistance.

v. Customer shall abide by the tips and safeguards mentioned on the Bank's website on Secured Banking available at https://www.obcindia.co.in/content/deposit-security-alert. Customer shall go through various instructions and awareness communication sent by the bank on secured banking

vi. Customer should make use of various features like card control and also set transaction limits to ensure minimized exposure.

vii. Customer should verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

F. REPORTING OF UNAUTHORIZED TRANSACTION BY CUSTOMERS TO BANK

Banks sends alerts through SMS to the customer for the financial transactions undertaken by them in their accounts using the electronic channels.

The SMS alerts shall be mandatorily sent to the customers having registered mobile number while Email Alerts shall be sent to customers having their E-Mail ID registered with the Bank.

The customers are required to inform or notify the Bank about the unauthorized/ fraudulent transactions upon receipt of such alerts through a Fraud Reporting Form (Copy enclosed as **Annexure I**) in their parent branch accompanied FIR/Police Complaint (for single or multiple transactions) and a duly signed written complaint depicting the disputed transactions, brief information describing the fraud along with supporting proof if any which would help in bank's internal investigation.

Notification of unauthorized/ fraudulent transaction

The Bank shall provide following facilities to the customer for lodging their complaint for unauthorized/ fraudulent transactions through electronic channels:

a) **Toll free number,** for reporting 'Unauthorized/ fraudulent' electronic transaction to be communicated in all the alerts for transactions sent to the customers. For any Electronic Transactions, a SMS to customers shall be sent appended with script "If txn. not done by you, call 18001801235" The customers may contact the 'Customer Care centre' toll free number for reporting of the unauthorized transaction.

   A complaint number shall be allotted to the customer acknowledging the notification of the unauthorized/ fraudulent transaction during the call for records in case of lost mobile number/ compromised mobile numbers.

b) **Parent/ Home Branches,** the customer can lodge the complaint for 'Unauthorized/ fraudulent' electronic transaction through parent/ home branch and receive the acknowledgement of the complaint. Such complaint shall be obtained through specified form for reporting of such unauthorized/ fraudulent transaction as per form mentioned above.

c) **Website:** The customer can lodge the complaint for 'Unauthorized/ fraudulent' electronic transaction through Bank website through link "Report

unauthorized electronic transactions" on homepage, wherein customer can directly report any unauthorized/fraudulent electronic transaction. Instant Acknowledgement SMS is also sent to the customer with registered complaint number on customer Mobile number and status of complaint can also be viewed through Complaint status tab available on homepage of our bank's website under direct link "Report Unauthorized Electronic Transactions".

Upon notification of the complaint, if Bank initiates the 'Debit Freeze' in the account, then Bank shall not be liable for return of any cheque/ instrument/ mandate presented in the account during the period of freeze. The customer shall take adequate measure for making good on such cheque/ instrument/ mandate at their own cost & expenses.

G. CUSTOMER LIABILITY & COMPENSATION FOR UNAUTHORIZED ELECTRONIC TRANSACTIONS

The customer liability shall be determined in case of unauthorized/ fraudulent transaction on the basis of deficiency on the part of Bank or customer or anywhere else in the system, which is as under:

i. "Zero Liability" of a Customer

A customer is entitled to "Zero Liability" where the unauthorized transactions occur in the following events:

- Contributory fraud/ negligence/ deficiency on the part of the Bank, irrespective of whether or not such transaction is reported by the customer.

- Third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and customer notifies the Bank within **"Three (3) Working days*"** of receiving the communication/ transaction alert from the bank regarding such unauthorized transactions.

- Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer.

ii. "Limited Liability" of a Customer

The customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

- In cases where the loss is due to negligence or contributory negligence by a customer *(i.e. where the injured party has failed to act prudently)*, such as where he has shared the payment credentials; the customer will bear the entire loss until he reports the unauthorized transaction to the bank.

  Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

- In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of **four (4) to seven (7) working days*** after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount summarized in the table below:

Table-1

Sl.	Type of Accounts	Max. liability of customer
1.	BSBD Accounts *(SB212, SB216, SB222, SB224, SB228 & OD521)*	₹5,000/-
2.	All Savings Bank accounts	₹10,000/-
3.	Current/ CC/ OD accounts of MSMEs	₹10,000/-
4.	Current/ CC/ OD accounts of Individuals with annual avg. balance/ sanction limit up to ₹25.00 Lacs *(during 365 days preceding the incidence of fraud)*	₹10,000/-
5.	Prepaid payment instruments (PPIs)	₹10,000/-
6.	All other Current/ CC/ OD accounts	₹25,000/-

**Working day to be computed in accordance to point no. V.(b).iii*

- In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay of **beyond Seven (7) working days to Ten (10) working days** after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, then the Bank may at its discretion decide to compensate a maximum of 25% of such unauthorized amount subject to a

maximum of ₹25,000/- per transaction irrespective of the customer account type.

iii. Complete Liability of customer:

- In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay of **beyond Ten (10) working days** after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, then the **Bank shall not be liable** to compensate any of such unauthorized transaction amount.

- Customer shall bear the entire loss in cases where the loss is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account/Transaction details, viz. Internet Banking user Id & PIN, Debit/Credit Card PIN/OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attack. This could also be due to SIM deactivation by the fraudster. Under such situations, the customer will bear the entire loss until the customer reports unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by the bank.

- Customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card hot listed or user blocked or does not cooperate with the Bank by providing necessary documents including but not limited to police complaint and submit fraud reporting or dispute form.

- If the bank learn or understand in due course/ later of internal investigation or from insurance investigator/ assessor/ valuer report or law enforcement agency report that the fraudulent transaction loss was crystallized due to forceful disclosure of e-channel credentials out of a criminal offence or civil offence of a family dispute then any compensation given to the customer will be debited to the customer account and credited back to the Bank.

H. REVERSAL TIMELINES FOR ZERO/ LIMITED LIABILITY OF CUSTOMERS

On being notified by the customer within ten (10) working days of such unauthorized electronic transaction, the bank shall credit (under **lien or shadow reversal with value date**) the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from **the date of such notification** by the customer *(without waiting for settlement of insurance claim, if any).*

The credit shall be value dated to be as of the date of the unauthorized transaction.

Thereafter, Bank shall investigate the matter for establishing the liability of the customer, if any. The resolution of the customer notification of the unauthorized electronic transaction shall be completed in a time bound manner, wherein:

iii. In case complaint is resolved and customer liability, if any, is established **within 90 days** from the date of receipt of the complaint, then the customer shall be compensated as per provision in section V.(g).

iv. Wherever the Bank is unable to resolve the complaint or determine the customer liability, if any, **within 90 days**, then the compensation shall be paid to the customer as per provision in section V.(g).

However, if the customer notifies the Bank beyond ten (10) working days from the date of such unauthorized electronic transaction, then Bank shall not afford any credit (under lien or shadow reversal) to the customer for such reported unauthorized transactions.

I. FORCE MAJEURE

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities, absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

ANNEXURE III

LIST OF ACRONYM

2 FA	Two Factor of Authentication
A-PIN	Application PIN
ATM	Automated Teller Machines
BC/ POT	Business Correspondent (Handled POT machines)
BHIM	Bharat Interface for Money
BSBDA	Basic Saving Bank Deposit Account
CA	Current Account
CBS	Core Banking System
CCA	Cash Credit Account
CNP transactions	Card Not Present Transactions
CP transactions	Card Present Transactions
CVV	Card Verification Value
e-Channel	Electronic Channels
ECI-7	E-Commerce Identifier 07 *(Used by Visa for International eCommerce transactions)*
e-Commerce	Electronic Commerce
E-mail	Electronic Mail
EMV	Europay MasterCard and Visa
FIR	First Information Report
IMPS	Immediate Payment Services
IP	Internet Protocol
Login Credentials	User IDs, User Name, Passwords or PINs
M-PIN	Mobile PIN
NEFT	National Electronic Fund Transfer
NFC	Near Field Communication
NI Act	Negotiable Instruments Act
ODA	Overdraft Account
OTP	One Time Password
PCIDSS	Payment Card Industry Data Security Standards
PIN	Personal Identification Number
POP	Point of Purchase
POS	Point of Sales
PPIs	Prepaid Payment Instruments
QR	Quick Response
RTGS	Real Time Gross Settlement
SBA	Savings Bank Account
SIM	Subscriber Identification Module
SMS	Short Message Service
UPI	Unified Payment Interface
User ID	User Identity
W.e.f	With Effective From

*****