Customer Protection Policy

Unauthorized Electronic Banking Transactions

(01-10-2018)

Payment & Settlement Department, Corporate Headquarters, M.A. Road Srinagar - 190001

Index of Topics covered in Policy

Definitions of some important abbreviations covered in policy.

ATM	:	Automated Teller Machine used for cash withdrawal through Credit and Debit Cards.
POS	:	Point of Sales Terminal installed at Merchant Establishments/shops for accepting payments through Plastic Cards.
CP	:	Card Present Transactions that require use of physical card at ATM POS.
CNP	:	Card Not present Transactions that do not require physical use of card like transactions carried on internet (e-com transactions).
PPI	:	Prepaid Payment instruments (PPI) like pre-paid and gift cards.
PCIDSS	:	Payment Card Industry Data Security Standards, certification required for card personalization, card data storing and processing.
ISO	:	International Organization for Standardization.
VAPT	:	Vulnerability Assessment and Penetration Testing for ensuring system and Data security.
eFRM	:	Electronic Fraud Management , a tool used for timely detection of fraud.
PIN	:	Personal Identification number, used as Password for carrying transactions at ATM.
CVV	:	Card verification Value, 3 digit secret code mentioned at the backside of card and used for performing e-com transactions.
OTP	:	One time Password, received on registered mobiles for finalizing a transaction.
3DSecureCode	:	Secondary level password generated by customers for online transactions.

==========

1. Introduction

The Banking industry has seen huge transformation from paper based payment system to electronic payment system and usage of different variants of plastic cards through three major delivery channels viz ATM, POS and internet has increased manifold in recent times. Moreover, with the introduction of new electronic payment channels like E-banking, Mobile banking the variety of choices has increased for customers to perform the transactions in an electronic mode.

Bank is committed to provide a secured environment to its customers for using electronic / digital mode of payment and has taken a number of fraud prevention / mitigation measures In this regard.

With the increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to customers' accounts, the criteria for determining the customer liability in these circumstances have been reviewed by RBI and they have advised revised directions vide their circular DBR.No.Leg.BC.78/09.07.005/2017-18 dated 06-July-2017.

2. Objective

The policy has been framed in line with RBI guidelines to cover the following aspects:-

a) Customers' liability in cases of unauthorized electronic Banking transactions occurring due to third party breach / customer negligence / Deficiencies on part of the Bank.

b) Customer compensation due to unauthorized electronic Banking transaction within defined timelines.

c) Customer protection by evolving the Banking system to provide secured environment for customers to use electronic mode for carrying transactions and creating a proper mechanism for customer awareness on the risks and responsibilities involved in electronic Banking transactions.

3. Scope

The policy covers following two categories of electronic banking transactions:-

(i) **Remote/online payment transactions** (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card not present(CNP)transactions, Pre-paid Payment Instruments (PPI), and

(ii) **Face-to-face/ proximity payment transactions** (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

4. Strengthening of systems and procedures:

It is the need of the hour that the systems and procedures in the Bank must be designed to make customers feel safe about carrying out electronic banking transactions. RBI to this effect has circulated certain key parameters which are to be addressed on top priority. The details whereof with initiatives to be taken at Bank level to comply to the guidelines are documented hereunder;

RBI Advisory	**Initiatives to be taken by Bank.**
a) To put in place appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers.	Information Systems (IS) Security should initiate steps for Payment Card Industry Data Security Standards (**PCI DSS)** certification in addition to timely renewal of International Organization for Standardization (**ISO) certifications**. The internal IS audit of the Bank should also take into consideration the checklist applicable for these two certifications. This shall ensure that the desired procedures and processes are being followed in letter and spirit. In addition to this Vulnerability Assessment and Penetration Testing (**VAPT**), a technical assessment process to find security bugs in a software

	program or a computer network, should be got conducted at regular intervals and compliance to observations if any sought within the minimum possible time frame.
b) Put in place robust and dynamic fraud detection and prevention mechanism	Bank should procure Electronic Fraud Risk Management **(eFRM)** solution for ensuring timely detection of frauds with robust mechanism. Furthermore, ASP based FRM solution from MasterCard and National Payments Corporation of India (NPCI) needs to be monitored and reviewed regularly by **Transaction Monitoring Cell (TMC).**
c) Put in place a 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	Integrated Risk Management Department (**IRMD**) to put in place the necessary mechanism and do the impact/scenario analysis.
d) Put in place appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom.	**A)** For this purpose, the bank should explore taking a comprehensive "**Cyber Insurance Policy**". **B)** In case the quotes so obtained from the insurance vendor are found to be on higher side, setting up of an **"Internal Fund"** for settlement of such claims can also be explored. A more detailed explanation of the Insurance policy is explained in coming paras under "**Hedging of Bank's Risks".**
e) Put in place a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.	Bank through its Corporate Communication Department should launch information campaigns / customer awareness drives on regular basis and utilize print / electronic media for the same. The customers can also be advised on how to protect themselves from electronic banking and payment related frauds through other modes of communications like

	SMS, emails and Bank's website and guided to avoid sharing of sensitive information viz user IDS , passwords, Card numbers, Card Expiry Date, PIN, CVV , OTP/ 3D Secure code, date of birth etc. .

5. Liability of a customer

Customer Liability in case of unauthorized electronic Banking transactions shall be determined as under:

a) Zero Liability of a customer

A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs due to following:-

i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.

b) Limited Liability of a Customer

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

i) Where the loss is due to negligence by a customer, such as where he has shared the payment credentials viz user IDs, Password / 3D Secure Code, PIN, OTP (one time password), Card Number, Expiry Date, CVV number, Date of Birth etc. 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.

ii) A customer shall be liable for the loss occurring due to unauthorized transactions 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 to seven 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 mentioned in Table 1, whichever is lower;

Table 1

Type of Account	**Maximum liability of customer**
Basic Saving Bank Deposit (**BSBD**) Accounts	**5,000**
All other SB accounts Pre-paid Payment Instruments and Gift Cards Current/ Cash Credit / Overdraft Accounts of MSMEs Current Accounts / Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs.25 lakh Credit cards with limit up to Rs.5 lakh	**10,000**
All other Current / Cash Credit / Overdraft Accounts Credit cards with limit above Rs.5 lakh	**25,000**

c) Complete liability of customer

i) In cases where the responsibility of 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 on part of customer in reporting to the Bank beyond **seven working days**, the customer would be completely liable for all such transactions.

6. Hedging of Bank's Risks (Risk Mitigation):

As provided at Clause 5 above, RBI while classifying the electronic transactions has also put a cap on the customer liability. This warrants for having in place a mechanism for hedging the risks so that bank's interests are also safeguarded.

One option is that of having in place an Insurance program so as to cover all losses due to frauds in such transactions. The various claims on account of customer liability fixed by Reserve Bank of India can be settled through such Cyber Insurance policy wherever required. As an alternative, in case the quotes so obtained from the insurance vendor are found to be on higher side, setting up of an internal fund for settlement of such claims can also be explored. The various scenarios discussed at Clause 5 for determining the customer Liability in unauthorized electronic banking transactions can be brought under Insurance coverage as under:-

a) All instances mentioned above at clause 5 (a) are to be fully insured. Any loss due to such instance has to be fully protected. However, Bank in as per laid down norms of the associations / good faith will take up the matter with all concerned in the system and the amount of claim shall be less by any reimbursements Bank may receive from any of the concerned party in the echo system of the transaction.

b) As per aforesaid clause 5, b (I) customer is liable for the entire amount of loss till the time customer reports the incident to the Bank therefore any losses occurring after the reporting by customer due to a system lapse at Bank side have to be borne by the Bank and same needs to be insured fully.

c) As per Clause 4, b (II) any amount beyond the limits set by RBI for customers has to be fully insured. The amount of claim in this case shall be the total amount of fraud less by the amount of liability passed on to the customer.

d) As per abovementioned clause 4, C (I) customer shall be completely liable for all unauthorized electronic banking transactions due to reporting by customers to the Bank beyond seven working days. However, in cases wherein the matter is referred to the court of law and the judgment is passed in favor of the customer, the amount involved has to be reimbursed by the insurance agency.

7. Reversal Timeline for Zero Liability / Limited Liability of customer:

a) On being notified by the customer, the bank through its Payment & Settlement Department shall credit (shadow reversal, meaning customer will not be able to use the funds by way shadow credit till the dispute is resolved in favour of the customer) 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.

b) Payment & Settlement department of the Bank shall ensure that complaint is resolved and liability of the customer, if any, established usually within 45 days, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated wherever warranted as per relevant provisions of this document.

c) Where the Bank through its authorized department is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in this document is paid to the customer, which shall include value dated interest/charges recalculations also.

8. Reporting and Monitoring

a) Payment & Settlement Department shall put in place a mechanism for the reporting of the customer liability cases to IT Strategy Committee of Board. IT Strategy committee of the Board should analyze the individual cases / incidents and take necessary measures wherever required for curbing/controlling the Frauds.

b) The reporting shall, *inter alia*, include volume/ number of cases and the aggregate value involved and distribution across various categories of cases viz., card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions, etc.

c) Payment & Settlement Department shall submit the report about reported unauthorized banking transactions to Standing Committee on Customer Service on quarterly basis through Customer Care Division. The Standing Committee on Customer Service shall review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redress mechanism and take appropriate measures to improve the systems and procedures.

d) All such transactions shall be reviewed by the bank's IS Audit as well.

e) Payment & Settlement Department shall be nodal office for reporting such transactions to all the departments as warranted in this document. Once a transaction is identified as a fraud, Payment & Settlement Department after collecting all the evidences shall forward the case to Vigilance department for further investigation and disposal.

f) However, as far as reimbursing the amount due to the customer is concerned this shall be the sole responsibility of Payment & Settlement Department.

9. Other Roles and Responsibilities of the Bank:

a) Bank shall ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.

b) The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever email ID is registered with Bank.

c) The customers must be advised to notify the bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction and informed that the longer the time taken to notify the bank, the higher will be the risk of loss.

d) To facilitate this, bank must provide customers through Contact Centre with 24x7 access through multiple channels (at a minimum, via phone banking, e-mail, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and / or loss or theft of payment instrument such as card, etc.

e) Bank shall not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank.

f) On receipt of report of an unauthorized transaction from the customer, bank shall immediately hotmark / block transactions in the account through electronic channels. These shall only be allowed once fresh ids/cards etc. are issued to the customer.

g) Ongoing customer education and freezing of formats for various SMS alerts regarding safety and security of electronic transactions shall be the responsibility of TMC and Information Security Departments of the Bank.

h) Bank shall provide a direct link for lodging the complaints with specific option to report unauthorized transaction in the home page of the Bank's website and provide an alternate standard number on which dispute may immediately be logged through a short SMS such as "YES/NO". The loss / fraud reporting system should also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by banks to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability. The latest directions from RBI in this regard shall be implemented immediately.

10. Obligations of Customer:

a) Customer shall mandatory register his/her valid mobile number with the Bank for availing SMS alert service and shall update his / her contact details as an when same are changed.

b) For the purpose of investigation, customer shall immediately surrender the card at Issuing Branch of the Bank in case of card present transaction and provide the customer dispute form in the prescribed format.

c) Customer shall also lodge FIR with police authorities and forward the copy of same to the Bank.

d) Customer shall provide any other relevant documents which would help Bank's investigation Team for the completion of investigation process and provide all assistance to the Bank Team as and when required.

e) Customer shall ensure confidentiality of sensitive card / account details viz user IDs, Passwords, Card Number, Card Expiry Date ,PIN, CVV, OTP/3D Secure +Code and shall never share the same with any known or unknown persons / entities, including bank staff.

f) Customer shall take all other necessary preventive measures, communicated from the Bank through SMS Alerts, emails, Print / electronic Media and through other public awareness campaigns for safeguarding various electronic devises/Cards from the intrusion of external hands/hackers.

11. Delegation of Powers and Reversal Process

i) The per card delegation of powers for reversal of disputed transaction amount to customer's account shall be as under:-

Amount in Rs.

Approving Authority	Approving limit (per card)
a) Chairman	**Above 50000**
b) President	**25001 to 50000**
c) Vice President	**10001 to 25000**
d) Incharge P&S Deptt	**Upto 10000**

ii) The following steps shall be taken by Payment & Settlement Department while reversing the disputed transaction to customer's account:

a) The transaction shall be reversed (shadow reversal) by debit to Suspense account within 10 days from the date of 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.

b) The claim shall be lodged with Insurance Company within 10 days from the date of receipt of customer complaint regarding unauthorized electronic transaction in case of availability of Cyber Insurance Policy.

c) The Insurance Company shall settle the claim within 30 days.

d) Incase Bank has created an internal fund for settling of customer claims the transaction shall be reversed by debit to said Insurance Fund.

iii) The suspense should be washed off within 45 days by following way:

a) Suspense shall be adjusted by the proceeds received from Insurance Company In terms of Cyber Insurance Policy and case forwarded to Vigilance Department for further investigation and disposal.

b) In case Cyber Insurance Policy is not available or there is no insurance coverage / Internal Fund available against specific type of Fraud Incident the suspense be adjusted by debit to P&L after due diligence but within 90 days.