Payment & Settlement System (PSS)

Customer Protection Policy

(Unauthorized Electronic Banking Transactions)

Version 2.0

Payment & Settlement Department
Corporate Headquarter, M. A. Road, Srinagar
+91- 0194-2481970; 2481903; 2481979; 2481966
chargeback.atm@jkbmail.com
chargeback@jkbmail.com; atm.fraud@jkbmail.com

Document Control & Version History

Title	Customer Protection Policy (Unauthorized Electronic Banking Transactions)	Version No.	2.0
Created By	Payment & Settlement Department	Date of Creation	11-11-2020
Reviewed By	ORMC	Date of Latest Review	20-11-2020
Approved By	Board of Directors	Date of Approval	29-12-2020
Date of Next Review			January 2022

Index of Topics covered in Policy

Glossary - Definitions of Some Important Abbreviations Covered in Policy

Abbreviation	Definition
ATM	Automated Teller Machine used for cash withdrawal through Credit and Debit Cards
POS	Point of Sales Terminal installed at Merchant Establishments/shops for 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.
PCI-DSS	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.
e-FRM	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.
3D-Secure Code	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 online (E-com) has increased manifold in recent times. Moreover, with the introduction of new payment E-channels like E-banking, Mobile Banking, UPI, IMPS the variety of choices has increased for customers to perform the transactions in an electronic mode.

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

Adhering to RBI guidelines on customer protection, JK Bank is committed to provide a secured environment to its customers for using electronic / digital mode of payments and has taken a number of fraud prevention / mitigation measures in this regard.

2. Objective

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

a) Customer's 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(s) 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

i) To cover the risks arising out of unauthorized debits to customer accounts owing to customer negligence / bank negligence / banking system frauds / third party breaches, banks need to clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios.

ii) To cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorized electronic banking transactions.

iii) To be transparent, non-discriminatory and shall stipulate the mechanism of compensating the customers for the unauthorized electronic banking transactions and also prescribe the timelines for effecting such compensation.

4. Strengthening of systems and procedures

The electronic / digital transactions are broadly divided into two categories.

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, UPI, IMPS and 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.)

The systems and procedures in the bank shall be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, Bank shall put in place:

i. Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;

ii. Robust and dynamic fraud detection and prevention mechanism;

iii. 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;

iv. Appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and

v) A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

In this regard to promote safe digital transactions among the general public, bank shall reiterate below appended instructions through Print / Electronic / Social media:

a) Register your mobile number and email with the bank to get instant alerts;
b) Not to share with anyone Card (Debit / Credit / Prepaid) details ;
c) Not to share password, PIN, OTP , CVV, UPI-PIN etc.;
d) To avoid undertaking banking or other financial transactions through public , open or free wifi-networks;

e) Not to store important banking data on mobile, e-mail, electronic wallet or purse. Customer may remember that bank nerve ask for details such as password, PIN, OTP, CVV number ;
f) Change your online banking password / PIN, Block your Debit / Credit / Pre-paid Card immediately, if it is lost or stolen.

Further, following internal initiatives shall be taken as part of customer awareness program;

i) This Policy Guideline on Customer Protection shall be published on Banks website and linked with already existing Citizen Charter.

ii) Business Units shall be advised to designate a helpdesk at their respective places to guide / educate the customers about various risks and responsibilities involved in digital transactions.

iii) Corporate Communication Dept. shall arrange displaying posters based on do's and don'ts as per above mentioned instructions at v(a to f).

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 will be liable for the loss occurring due to unauthorized transactions in cases where the responsibility for the authorized 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 (Rs.)**
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 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 Lacs Credit cards with limit up to Rs.5 Lacs	**10,000**
All other Current / Cash Credit / Overdraft Accounts Credit cards with limit above Rs.5 Lacs	**25,000**

c) Complete Liability of a Customer

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 in line with current Policy guidelines and as per directions of RBI vide circular no. DBR.No.Leg.BC.78/09.07.005/2017-18 dated 06-July-2017.

For determining the customer liability, the number of working days shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

6. Reversal Guidelines and Timeline for Zero Liability / Limited Liability of customer

a) On being notified by the customer, the bank through its Payment & Settlement Department shall give shadow credit (meaning customer will not be able to use the funds by way of shadow credit till the dispute is resolved in favor 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 or otherwise). The credit shall be value dated to be as of the date of the unauthorized transaction.

b) Payment & Settlement Department shall ensure that complaint is resolved and liability of the customer, if any, is 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. Further, on case to case basis Bank may at their discretion decide to waive off any customer liability in case of unauthorized electronic banking transactions even in cases of customer negligence.

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 shall be paid to the customer, with value dated interest/charges recalculations also.

d) Payment and Settlement Department after settling the reported fraud case and before releasing the shadow credit in favor of the customer, shall ask for indemnity bond from the customer , as per pre-defined format available with the department. The indemnity bond shall require the Card Holder to UNDERTAKE AND AGREE to INDEMNIFY the Bank and keep it indemnified against all claims, demands, proceedings, losses, damages, charges and expenses which bank may suffer or in consequence of BANK

having agreed to pay/or paying CARD HOLDER, the said sum, as reported fraud, in case the investigations of the Law Enforcement Agency came to the Conclusion /establish that the transactions were not fraudulent , or were made on account of any lapse/negligence/Convenience on part of the Card Holder.

7. Reporting and Monitoring

a) Payment & Settlement Department shall put in place a mechanism for the reporting of the customer liability cases to Audit Committee of Board (ACB) on quarterly basis. ACB shall 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, UPI, IMPS, Credit Card and Debit Card ATM transactions, etc.

c) The Standing Committee on Customer Service shall periodically 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 shall take appropriate measures to improve the systems and procedures. All such transactions shall be reviewed by the bank's internal auditors.

8. 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 burden / responsibility of proving customer liability in case of unauthorized electronic banking transactions shall lie on the bank.

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

d) 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.

e) To facilitate this, bank shall 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.

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

g) On receipt of report of an unauthorized transaction from the customer, bank shall immediately hot mark / block transactions in the account through electronic channels or will totally debit freeze the account as per the nature of fraud with the consent of customer. The transaction through ATM shall be allowed only after new / fresh debit card is issued to the customer.

h) Ongoing customer education and freezing of formats for various SMS alerts regarding safety and security of electronic transactions shall be the responsibility of bank through Corporate Communication, Transaction Monitoring Cell (TMC) and Information Security Departments.

i) Bank shall provide the details of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts.

j) Banks shall also display their approved policy in public domain for wider dissemination. The existing customers shall also be individually informed about the bank's policy.

k) On receipt of report of an unauthorized transaction from the customer, bank shall take immediate steps to prevent further unauthorized transactions in the account.

l) Bank shall provide a grievance redressal link for lodging the grievances 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 shall 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. All the directions from RBI in this regard shall be implemented from time to time.

9. 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. Further, customer shall inform bank with new number in case existing mobile number on which SMS alert service has been subscribed is not having national roaming.

b) For the purpose of investigation, customer shall immediately surrender the card at Issuing or any other nearest branch of the Bank in case of fraud on card present transaction and also 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 shall also 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 , social media and through other public awareness campaigns for safeguarding various electronic devices/Cards from the intrusion of external hands/hackers.

10. Delegation of Powers and Reversal Process

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

Amount in Rs.

Approving Authority	Approving Limit (Per card)
Chairman	Above 1.00 Lacs
Executive President	Above Rs.0.50 Lacs to Rs.1.00 Lacs
President	Above Rs.0.25 Lacs to Rs.0.50 Lacs
Vice President	Above Rs.0.10 Lacs to Rs.0.25 Lacs
In charge P&S Dept.	Upto Rs.0.10 Lacs

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, or otherwise 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) In case insurance cover is not available and Bank has created an internal Corpus Fund for settling of customer claims, the transaction shall be reimbursed by debit to such Corpus Fund.

d) However, in case there is no insurance cover nor any corpus fund has been created by the bank, then transaction amount shall be reimbursed by debit to Operation Loss account, after seeking approval from concerned approving authorities as per delegation of powers mentioned above.

iii) The suspense if any raised shall 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.

b) In case Cyber Insurance Policy is not available or there is no insurance coverage / Internal Fund i.e., Corpus Fund available against specific type of Fraud Incident, the suspense be adjusted by debit to Operational Loss Account after due diligence but within 90 days.

11. Ownership and Review

Ownership of the policy shall remain with Payment and Settlement Department of the Bank. The policy shall be subject to annual review. The review of the policy will be put up to Board for approval. Approved revised policy & guidelines will remain in force till next review.

In case of exigencies and to be in line with regulatory / statutory guidelines, the Chairman / Managing Director is empowered to approve changes /modifications/ amendments/ relaxations/ exemptions, if any, required to be made in the policy and same will be submitted to the Board for ratification .

Any guideline(s) issued by regulators with regard to Customer Protection (Limited Liability) Policy or any other matter dealt with by this Policy will be deemed to be part & parcel of this policy for operational purpose with immediate effect. A note regarding such directive should be placed before Board for information.

12. Disclosure of the Policy

In addition to the internal circulation of the policy through Banks intranet, the policy shall also be displayed on the web site of the Bank.

The Jammu and Kashmir Bank Limited Corporate Headquarters, M. A. Road, Srinagar 190001, Kashmir (J&K)
www.jkbank.com,www.jkbank.net