भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

NPCI / 2021 – 22 / RMD / 004

01 September 2021

To,

All Member banks, AePS

Respected Madam / Dear Sir,

Sub: Aadhaar Enabled Payment System – Fraud Liability Guidelines

In the AePS Fraud and Risk Working Group meeting held on 21st February 2019, the guidelines for handling fraud transactions in AePS and liability arising there from, were discussed and agreed upon. Accordingly, in the 25th AePS Steering Committee meeting held on 19th March 2019, the same was agreed to be implemented in order to deal with fraudulent transactions. It was also agreed that members will adhere to formal fraud and risk guidelines rolled out in this regard. The guideline for handling fraud transactions in AepS are detailed in **Annexure A** (hereinafter referred to as "**Guideline**").

Members are requested to note the following key features of the Guideline:

1. The Guideline will be applicable for all financial transactions in AePS (Viz., Cash withdrawal, Cash Deposit, Funds transfer and BHIM Aadhaar) involving Business Correspondents (BC), BC agents or Customer Service Points (CSP).
2. NPCI's role will be limited to facilitate the process of reporting and handling of fraud transactions between the members and oversee the adherence to the Guideline by the members. In case of any contravention, compromise or breach of the processes, specifications, guidelines laid down by Unique Identification Authority of India (UIDAI) or Aadhaar data including capturing and securing of biometric information of the Aadhaar number holder, the same will be dealt with by UIDAI in accordance with the extant rules and regulations of UIDAI and laws as applicable in this regard.
3. All members shall discharge their respective responsibilities prescribed under the Guideline, and adhere to the Guideline.
4. The Guideline may be updated by NPCI, from time to time, in accordance with the directions of the AePS Steering Committee.
5. The Guideline are in line with the discussions held in the AePS Fraud and Risk Working Group meeting dated 15th July 2021.

Members are requested to circulate the Guideline to all relevant departments within their respective organizations.

Any query or clarification sought in regard to the Guideline may be referred to aeps.fraudrisk@npci.org.in

Yours sincerely,

Sd/-
Viswanath K
Chief Risk Officer

Encl:

1. Annexure A - Guideline for handling fraud transactions under AePS
2. Annexure 1 - Issuer Investigation Report
3. Annexure 2 - Acquirer Investigation Report
4. Annexure 3 – Business Correspondent Negative Registry

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Annexure A

GUIDELINE FOR HANDLING FRAUD TRANSACTIONS UNDER AePS

This guideline provides the process for handling fraudulent transactions performed in AePS and to determine financial liability of the members inter se, with respect to such transactions. This process is being set up in order to facilitate the members to handle fraud transactions between themselves.

The process envisaged hereunder will help determine whether the fraud or error resulting in a fraudulent transaction in AePS was committed by the acquirer bank, issuer bank or any of their respective Business Correspondent (BC), BC agent or Customer Service Point (CSP). If the fraud or error has been committed by the acquirer bank or it's BC, BC agent or CSP, the acquirer bank shall accept the responsibility of such fraud or error in AePS and refund the transaction amount to the issuer bank. If the fraud or error has been committed by the issuer bank, its BC, BC agent or CSP or its customer, then the issuer bank shall accept the responsibility of such fraud or error and accordingly, it will not be entitled for refund of transaction amount from the acquirer bank and the issuer bank shall refund the transaction amount to the customer.

All members shall adhere to this guideline and follow the process detailed herein for reporting and handling any fraudulent transactions in AePS.

I. Process:

i. Upon receipt of intimation regarding a possible fraud transaction, the issuer bank shall notify NPCI of the same within 05 days from the date such transaction was reported to it by the customer, along with issuer bank's investigation report in the format prescribed in **Annexure 1** detailing the nature of the fraud and additional inputs, if any.
ii. NPCI will notify the fraud transaction to the relevant acquirer bank along with the investigation report submitted by the issuer bank.
iii. Acquirer bank shall investigate the reported fraud including with the relevant BC, BC agent or CSP, as the case may be, and provide its investigation report to NPCI in the format prescribed in **Annexure 2** along with the relevant supporting documents, within 10 days from the date it is in receipt of notification of fraud from NPCI. At this stage, the acquirer bank shall also provide NPCI the final resolution on the transaction i.e. whether the acquirer bank is, or is not, agreeable to bear the financial liability for such transaction.
iv. In case the acquirer bank accepts responsibility of the fraud or error, then it will refund the transaction amount to the bank account or pool account of the issuer bank mentioned in the issuer investigation report, within 03 days from the date NPCI was informed of such final resolution by the acquirer bank. Thereafter, issuer bank shall be responsible to refund such transaction amount to the relevant customer within 02 days from the receipt of the transaction amount in the pool account.
v. In case the acquirer bank does not accept responsibility of the fraud or error and is not agreeable to undertake the financial liability of the fraud transaction, the acquirer bank shall share with the issuer bank relevant documents to support its position in this regard, and to enable the issuer bank to validate such documents.
vi. Issuer bank shall verify the supporting documents and if, upon verification of the documents it is evident that fraud or error was committed by the issuer bank, or customer and / or in case of any other scenario as may be identified by NPCI in this regard, then the issuer bank will bear the financial liability for such fraud transaction. Accordingly, the issuer bank shall reimburse the transaction amount to the customer.

II. Liability Matrix

The following table provides the fraud transaction scenarios and the member who will bear the financial liability for the same. The scenarios given in the table below are not exhaustive and the same will undergo amendment, from time to time, as and when any new trend or fraudulent modus operandi is identified.

Sr. No.	Description	Rationale	Liability/ Responsibility
1	Delay in reporting fraud (beyond 90 days)	Time barred	Issuer
2	Wrong Aadhaar linking / seeding	UIDAI compliance requirement not met by issuer	Issuer
3	Customer involvement / collusion with BC / BC agent / CSP	Issuer investigation diligence not conducted	Issuer
4	Delay by the acquirer in resolving the fraud reported by the customer (beyond 10 days)	Investigation incomplete due to acquirer. Customer will be given the benefit of doubt	Acquirer
5	On boarded BC / BC agent / CSP name or details is present in the negative registry (**Annexure 4**)	Acquirer due diligence is not conducted	Acquirer
6	BC / BC agent / CSP is compromised and found to be colluding with fraudsters	Acquirer diligence on ongoing monitoring as per RBI guidelines*	Acquirer
7	Inconclusive acquirer investigation, BC / BC agent / CSP not reachable, contactable, or co-operative etc.,	Acquirer due diligence in terms of ongoing monitoring as per RBI guidelines	Acquirer

* Refer RBI/2010-11/217 DBOD.No.BL.BC.43 /22.01.009/2010-11 (https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=6017)

III. Fraud Classification:

The following fraud classifications will be considered for determining the liability under this guideline:

i. **Fake Bio-metric fraud** - BC, BC agent, CSP or other person uses victims' / customers' Aadhaar number, Virtual ID and fake biometric to perform financial transaction(s).
ii. **Deceiving customer to provide Aadhaar number, Virtual ID and / or Biometric** – BC, BC agent, CSP deceives the customer to provide the UID (Unique Identity Number) and biometric but ultimately uses it to perform financial transactions from the customer's account.
iii. **Wrong Aadhaar linking or seeding in account** - Issuer bank erroneously links wrong or another person's Aadhaar number in the actual customer's account. The person whose Aadhaar Number is incorrectly linked / seeded to the customer's / victim's account, misuses funds intentionally or unintentionally by performing financial transaction(s).
iv. **Others** – This includes other fraud types such as cheating fraud using social engineering techniques, BC, BC agent or CSP absconding, not available or is not contactable etc.

IV. Qualifying Criteria for Fraud Reporting : The criteria for reporting a fraud transaction under this guideline is detailed below:

i. Fraud reporting is mandatory. Issuer bank should report the fraud within 90 days from the date of the transaction.
ii. Issuer banks shall report only off-us transactions under this guideline.
iii. The reported transaction should be successful i.e. settled by NPCI. Failed transactions and declined transactions are not eligible for reporting as fraud transactions.
iv. Issuer bank should not have raised chargeback for the reported transactions.

V. Roles and Responsibilities:

The roles and responsibilities of the issuer bank, acquirer bank and NPCI under this process are as follows:

a) **Issuer Bank's Responsibilities:**
   i. Issuer bank should report fraudulent transactions to NPCI within 05 working days from the date the customer had reported the transaction to the issuer bank.
   ii. Issuer bank will submit the investigation report to NPCI on their letter head as per the format given in **Annexure 1.**
   iii. In case customer holds a joint account, issuer bank should mention names of all joint holders and their Aadhaar number (masked), in the investigation report.
   iv. Issuer bank will submit the investigation report along with the relevant transaction logs to NPCI at aeps.fraudrisk@npci.org.in.

b) **Acquirer Bank's Responsibilities:**
   i. On receiving the information about a fraud transaction, the acquirer bank should carry out complete investigation with respect to such transaction including on the role of the relevant BC, BC agent or CSP involved in the said transaction.
   ii. Within 10 working days from the date of receipt of intimation of fraud by the acquirer bank, it shall submit the duly filled up acquirer fraud investigation report on its letter head as per the format specified in **Annexure 2,** to NPCI at aeps.fraudrisk@npci.org.in along with the necessary transaction details, supporting documents or logs.
   iii. In case the acquirer fraud investigation report is not submitted to NPCI within the stipulated timeframe then the acquirer bank will be liable to bear the financial liability of such transaction.
   iv. The investigation report submitted by the acquirer bank should carry explicit confirmation on acceptance of financial liability or acquirer bank's rejection of the fraud claim submitted by the Issuer bank. Each rejection / refusal of the claim as set forth herein above shall be supported by adequate documents and records by the acquirer bank to substantiate / support the refusal.
   v. Acquirer bank shall also share additional supporting document or evidences in case where the BC, BC agent or CSP is confirmed as genuine (Customer dispute withdrawal letter, police complaint, evidence to prove customer collusion with agent, etc.)
   vi. In case repeat frauds are reported with respect to a particular BC, BC agent or CSP and no action is taken by the acquirer bank to block the terminal of the BC/BC Agent/CSP, then for all subsequent transactions, the financial liability for such fraud transaction shall be borne by the acquirer bank.
   vii. If the BC, BC agent or CSP is proven guilty of committing fraud, the acquirer bank shall terminate the services of such BC, BC agent or CSP, as the case may be, immediately and inform NPCI of the same along with an update to the BC negative registry (**Annexure 3**) within 48 hours from date of termination.

c) **NPCI Responsibilities:**

i. Within 2 working days from receipt of issuer bank investigation report, NPCI will notify the acquirer bank about the fraud transaction/period and the suspected BC, BC agent or CSP.

ii. NPCI will circulate the BC negative registry before 10th of each month until the BC registry is automated by NPCI. (Refer RMD Advisory dated 19th July 2021 - NPCI/2021-22/RMD/003)

iii. NPCI's role is limited to facilitate this process of handling fraud transactions and determining financial liability of the members inter se with respect to such transactions, and oversee the adherence to this guideline by the member banks. The decision of NPCI with respect to this guideline including any modifications therein, would be final and binding on the members.

VI. Third-party / Forensic Investigation:

i. In case of any breach / trend / incident at a BC, BC agent or CSP, NPCI, at its discretion, may direct the acquirer bank to empanel a third party/forensic investigators to conduct investigation.

ii. Whenever such investigations are warranted, the cost of such investigations will be borne by relevant acquirer bank and the acquirer bank will promptly share the report and outcome of such investigation with NPCI.

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Annexure 1

Format of Issuer Investigation Report

Fraud Analysis and Investigation Report		
ISSUER BANK INVESTIGATION		
1.	**CASE DETAILS**	
A.	Date of occurrence of fraud transaction	
B.	Date of fraud reported by customer	
2.	**CUSTOMER DETAILS**	
A.	Full name (mention names of all joint holders, if applicable)	
B.	Contact number	
C.	Masked Aadhaar number (masking all other digits of the Aadhaar numbers except the last four digits. For example: **** **** last 4 digits only) (mention Aadhaar numbers of all joint account holders, if applicable.)	
D.	Residential address	
	City	
	State	
	PIN CODE	
E.	Bank branch address	
3.	**TRANSACTION DETAILS**	
A.	Correct Aadhaar linking (Y/N)	
B.	Transaction type {Cash withdrawal, funds transfer, purchase transaction (Aadhaar pay), cash deposit}	
C.	Number of transactions reported	
D.	Total amount of reported transactions (in Indian Rupees)	
E.	Transaction date | acquirer ID | terminal ID | RRN number (12 digits as per BCS) | amount | timespan	
4.	**ISSUER INVESTIGATION DETAILS**	
A.	Has issuer bank received written fraud complaint letter from customer? (Y/N)	
B.	Is there any joint holder in customer's account? (Y/N)	
C.	Is the joint account holder aware of fraudulent transactions reported by the other account holder? (Y/N)	
D.	Customer's account type (savings/ current)	
E.	Has the customer shared his/ her biometric with any other entity/person for any purpose since the last 06 months? If yes, provide details.	
F.	Does the customer regularly carry out AePS transactions at same BC/BC agent/CSP locations?	
G.	Has the customer previously done any AePS transaction in last 06 months	

H.	How did the fraudulent transaction in the customer account come to the knowledge of the customer?	
I.	Customer's location at the time of transaction?	
J.	Was the customer's account statement checked for reported transactions?	
K.	Any other cases reported against the same BC/BC agent/CSP.	
L.	Action taken by Issuer Bank to stop subsequent AePS transactions in customer's account.	
M.	Is Aadhaar number delinked from the customer's account? (Y/N)	
N.	Is the customer's 'mobile number/ email id' updated in Aadhaar Card? (Y/N)	
O.	Is the customer's currently used mobile number updated with the bank for SMS alert? Also, was the same number used by customer at time of disputed transaction?	
P.	Was SMS message sent to customer's mobile number for reported transactions? If "No", provide the reason.	
Q.	Reason for late reporting of fraudulent transactions by customer (applicable for fraudulent transactions reporting done after 90 days from the date of transaction)	
R.	Whether Issuer Bank wants to report any other specific details.	

5.	**FIRST INFORMATION REPORT(FIR) DETAILS**	
A.	FIR/complaint lodged (Y/N).	
B.	If "No" provide reason	
C.	FIR number and date	
D.	Police station	
E.	Status of the case	

6.	**Account details for NEFT (in case of refund consent by acquirer bank)**	
A.	Name of the issuer bank:	
B.	Pool account name/ customer name in account:	
C.	Account number:	
D.	IFSC code:	
E.	Name of the branch:	

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Annexure 2

Format of Acquirer Investigation Report

Fraud Analysis and Investigation Report		
ACQUIRER BANK INVESTIGATION		
1.	**BC/BC agent/CSP DETAILS**	
A.	BC/BC agent/CSP Name and terminal ID	
B.	Contact number	
C.	Address	
D.	Date of on-boarding	
E.	Off-boarding/termination/suspension date (If applicable)	
F.	Exit reason	
G.	Corporate BC details (If any)	
2.	**ACQUIRER BANK INVESTIGATION DETAILS**	
A.	Is BC/BC agent/CSP contactable? If no, what action was taken by Acquirer Bank for reported AePS fraud?	
B.	Register maintained by BC/BC agent/ CSP (YES/NO). If YES, share details.	
C.	Did BC/BC agent/CSP collect any ID proof of the customer?	
D.	What was the location of the BC/BC agent/CSP on the date of disputed transaction?	
E.	Whether the BC/BC agent/CSP is working from a fixed location? If so, what is the location?	
F.	If the BC/BC agent/CSP is not working from a fixed location, wherefrom the BC/BC agent/CSP was operating during the last 06 months? Also share the locations.	
G.	Whether there are attempts, successful or failed by the BC/BC agent/CSP for the given Aadhaar number with multiple banks? If so the details thereof.	
H.	What is the procedure adopted by the acquirer bank for engaging the BC/BC agent/CSP?	
I.	What are the login guidelines adopted by the acquirer bank, for authenticating the BC/BC agent/CSP?	
J.	What are the transaction limits, daily limits set for the BC/BC agent/CSP?	
K.	Action taken by the acquirer bank to stop subsequent operation by BC/BC agent/CSP.	
L.	Is BC/BC agent/CSP involved in Fraud? (Y/N)	
M.	Any police complaint filed against BC/BC agent/CSP? (Y/N). If no, then the reason for the same.	
M1	If BC/BC agent/CSP is involved in fraud, has the BC/BC agent/CSP been added to the negative list and reported to NPCI	
M2	If the answer is "No" to M1, specify the reason	
N.	Fraud type (Fake biometric, wrong Aadhaar linking, siphoning fraud, others (with reason))	
O.	Brief description of the case/modus operandi	
P.	Is acquirer bank providing consent for refund to customer? (Y/N)	
Q.	Any other details with respect to reported transactions / case	

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Annexure 3

Format for sharing BC/BC agent/CSP information in Negative Registry

Field Name	Mandatory/ Non- Mandatory
BC/BC agent/CSP name	Mandatory
Address	Mandatory
City	Mandatory
State	Mandatory
Pin Code	Mandatory
Aadhaar No (**** **** last 4 digits only)	Mandatory
PAN No	Mandatory
Mobile No	Mandatory
Acquirer bank name which blacklisted the BC/BC agent/CSP	Mandatory
Date of blacklisting (Date Format: DD/MM/YYYY)	Mandatory
Reason for blacklisting (BC/BC agent/CSP involved in the fraud, absconding, not contactable/traceable, BC/BC agent/CSP - Customer collusion fraud, arrested for fraud)	Mandatory
Corporate BC name (If applicable)	Mandatory
BC/BC agent/CSP Terminal ID	Mandatory
Terminal Id	Mandatory
Bank name where BC/BC agent/CSP holds account	Optional
IFSC code where BC/BC agent/CSP holds account	Optional
Account number linked to blacklisted BC/BC agent/CSP	Optional
Is police complaint filed Y/N	Optional
If yes, FIR / compliant #	Optional
Date of the complaint (Format: DD/MM/YYYY)	Optional
Is the BC/BC agent/CSP arrested (Y/N)	Optional