

## Appendix

### CPFIR – Payment Fraud Reporting

The data collection file format is a combination of a single Header row and one or more data rows. The Header row is used to collect the metadata information about the data submitted by the reporting entity and data row contains details of the payment fraud reported.

### Header Format

Field Name	Field Length	Comments	Example
Return Code	3	Must be 'PFR' (Payment Fraud Reporting)	PFR
Flag	1	I – To identify the file has come for inserting the records for initial reporting U – To identify file has come for updating the records already reported	I or U
Reporting Entity Code	Upto 7 digit	As per the Centralised Information System for Banking Infrastructure (CISBI) of RBI	010
File Submission Date	8	Must be 'DDMMYYYY'	21012020
Record Count	20	Number of data rows present in the submitted file excluding header	1

#### Note:

- All individual fields must be separated by a colon (:).
- Header record must end with semi-colon (;)

#### Example:

PFR:I:010:21012020:1;

### Data Row Format

Field Name	Field Length	Mandatory (M) / Optional (O)	Guidelines	Comments
Internal identifier used by bank / non-bank entity	20	O	Alphanumeric field that can be used by reporting entity for their internal reference, if required.	Only alphanumeric, underscore, hyphen and multiple spaces are allowed.

Was the fraud reported by customer ?	1	M	If fraud reported by Customer – Y; If fraud detected by Bank / non-bank entity – N;	
Was it an attempted fraud ?	1	M	If attempted fraud – Y; Else – N;	
Payment transaction instrument used	3	M	Three digit code from the master data code list provided in Annex of this document.	
Payment system category	3	M	Three digit code from the master data code list provided in Annex of this document.	
System involved in the fraudulent transaction	10	M	System involved to be selected from the master data provided in Annex of this document.	
Payment channel used for fraudulent transaction	3	M	Three digit code from the master data code list provided in Annex of this document.	
Nature of fraudulent transaction	3	O	Three digit code from the master data code list provided in Annex of this document.	
Date of occurrence of the fraud as identified by the bank / non-bank entity	8	If Fraud Reported by Customer = No; M	Must be DDMMYYYY	
Date of detection of the fraud by bank / non-bank entity	8		Must be DDMMYYYY	
Date of entering in the system	8		Must be DDMMYYYY	
Date of occurrence of the fraud transaction reported by customer	8	If Fraud Reported by Customer = Yes; M	Must be DDMMYYYY	
Time of occurrence of the fraud	8		Must be HH:MM:SS	

transaction reported by customer				
Reporting date of fraud by the customer to bank / PPI issuer / PSO	8		Must be DDMMYYYY	
Date of entering the fraud by the bank / PPI issuer / PSO in the system	8		Must be DDMMYYYY	
Unique Transaction Reference No. of the fraudulent transaction	35	M	Unique Transaction Reference No. generated by the payment system that has processed the payment transaction. For attempted frauds that do not have any UTR, entities may specify ATTEMPTEDXXXX where XXXX is a sequence number.	Only alphanumeric, underscore and hyphen are allowed.
Is the fraud a domestic transaction?	1	M	If domestic transaction - Y; else - N;	
Reporting customer name	100	If Fraud Reported by Customer = Yes; M	Name of the customer	Only alphabets, numbers, dot, parentheses, single quote / apostrophe, ampersand, comma, hyphen, forward slash, back slash, underscore and multiple spaces are allowed.
Reporting customer mobile no.	15			Only numeric, single space, plus (1st char) and hyphen are allowed.
Reporting customer e-mail	50	O		Standard characters accepted in e-mail
Any other detail of the reporting customer	100	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi

				colon, forward slash and multi-spaces between them are allowed.
Was any PA / PG Involved ?	1	M	If PA / PG involved – Y; else – N;	
If PA / PG involved, the name may be provided	100	If PA / PG Involved = Y; M		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, parentheses, ampersand, back slash, @ sign, hash, + and multiple spaces are allowed.
Was any third party PSP involved ?	1	M	If third party PSP involved -Y; else N;	
If third party PSP involved, the name may be provided	100	If Third party PSP involved = Y; M		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, parentheses, ampersand, back slash, @ sign, hash, +, multiple spaces are allowed.
Amount involved (INR actuals) in the fraudulent transaction	20	If Attempted Fraud = N; M	Amount in rupees	Only numbers are allowed.
Amount recovered (INR actuals) in the fraudulent transaction	20	O	Amount in rupees	Only numbers are allowed.
Was insurance coverage available ?	1	O	If insurance coverage available – Y; else – N;	
Name of insurer and per transaction coverage amount	2000	If Insurance Coverage = Y; M		Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semicolon,

				parentheses, forward slash, dollar, euro, pound, rupee, krona, back slash, multiple spaces and line break are allowed.
Amount recovered due to Insurance cover	20	If Insurance Coverage = Y; M		Only numbers are allowed.
Beneficiary name	100	O	Name of the Beneficiary	Only alphabets, numbers, dot, parentheses, single quote / apostrophe, ampersand, comma, hyphen, forward slash, back slash, underscore and multiple spaces are allowed.
Beneficiary mobile	15	O		Only numeric, single space, plus (1st char) and hyphen are allowed.
Beneficiary e-mail	50	O		Standard characters accepted in e-mail
Beneficiary account number	50	O		Only numbers and alphabets are allowed.
Beneficiary bank	7	O	Bank Working Code from CISBI. For Non-Bank the code provided by DPSS	
Beneficiary branch (part 1 code)	7	O	Part 1 Code to be provided here as per the CISBI	
Beneficiary branch IFSC	11	O	IFSC for the Branch	Only numbers and alphabets are allowed.
Beneficiary PAN card no.	10	O		Only numbers and alphabets are allowed.

Beneficiary debit / credit card no.	16	O		Only numbers are allowed.
Beneficiary PPI card / wallet no.	50	O		Only alphabets, numbers, + and multiple spaces are allowed.
Beneficiary UPI ID	50	O		Only alphabets, numbers, @ sign, dot and hyphen are allowed in standard pattern.  @ is mandatory for UPI ID.  In case the transaction is based on UPI Number that should be entered. (@ is not required)
Name of destination PPI issuer	100	O		Only alphabets, numbers, hyphen, dot, single quote, colon, semi colon, forward slash, parentheses, ampersand, back slash, @ sign, hash, + and multiple spaces are allowed.
Destination merchant ID	50	O		Only alphabets, numbers, forward slash, parentheses, dot, ampersand, comma, colon, star, hash, underscore, single quote / apostrophe, + and multiple spaces are allowed.
Destination merchant name	100	O		Only alphabets, numbers, forward slash, parentheses, dot, ampersand, comma, colon, star, hash, underscore, single quote / apostrophe, +

				and multiple spaces are allowed.
Destination payment gateway / aggregator	50	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semicolon, forward slash, parentheses, Ampersand, Back slash, @, hash, + and multiple spaces are allowed.
Destination ATM ID	50	O		Only alphabets and numbers are allowed.
Suspect website used	100	O	Website address	Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, hash and no spaces are allowed.
Suspect mobile app used	100	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, hash and multiple spaces between them are allowed.
Suspect device ID	50	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, hash and multiple spaces between them are allowed.
Suspect IP Address	50	O		Only numbers, dot and colon are allowed.
Suspect IMEI number	20	O		Only alphabets and numbers are allowed.
Suspect geotag ID	50	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash

				and multiple spaces between them are allowed.
Any other details of suspect	100	O		Only alphabets, numbers, hyphen, dot, comma, single quote, colon, semi colon, forward slash, hash and multiple spaces between them are allowed.
Initial inputs on modus operandi of fraud	2000	O	Fraud related information, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Modus operandi – update 1	2000	O	Fraud related updates, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Modus operandi – update 2	2000	O	Fraud related updates, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces



				between them are allowed.
Modus operandi – update 3	2000	<input type="radio"/>	Fraud related updates, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Modus operandi – update 4	2000	<input type="radio"/>	Fraud related updates, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Modus operandi – update 5	2000	<input type="radio"/>	Fraud related updates, if any	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semi colon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
False alert – transaction was not a fraud	1	<input type="radio"/>	Must be Y/N, after investigation done	
Fraud was registered with Law Enforcement Agencies	1	<input type="radio"/>	Y/N to be provided	

(LEA) / sub-judice				
If fraud was registered with LEA, details of case reported	500	O	Details to be provided if the above field response is YES	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semicolon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Has the fraud incident been closed?	1	M	Must be Y/N	
Date of closure of fraud	8	If Fraud Closed = Y; M	Details to be provided if the above field response is yes in DDMMYYYY format	Date should be lesser than or equal to current date and greater than or equal to occurrence date as well as detection date.
Justification for closure of fraud	2000	If Fraud Closed = Y; M	Details to be provided if the above field response is yes	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semicolon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
Any other information pertaining to the fraud	2000	O		Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semicolon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.

Steps taken to address / prevent such frauds in future	2000	O	Only alphabets, numbers, hyphen, dot, comma, single quote, double quotes, ampersand, colon, semicolon, parentheses, forward slash, dollar, euro, pound, rupee, krona, line break and multiple spaces between them are allowed.
--	------	---	--

**Note:**

- Mandatory fields once submitted cannot be modified (except for fraud closed which can be updated from No to Yes).
- Once a fraud is closed, no updates are permitted.
- The output file generated for successful records shall contain a Fraud Reference Number (FRN) assigned to all successfully inserted records. The FRN shall begin with 'F' for actual frauds and 'A' in case of attempted frauds. The same FRN must be used for reporting Updates.
- The format for reporting updates is same as the format for initial reporting (Insert). Only the FRN generated during initial (Insert) reporting must be appended at the start of the record followed by pipe (|).
- Although some fields are marked as optional, entities are advised to report maximum available data to facilitate analysis and strengthen the ecosystem.
- All data elements to be separated by pipe (|).
- No additional character to be included at the end of each record.

**Example:** Insert record

```
CAN15112022000043446|Y|N|DEC|CAN|VISA|POS|OTH|||16112022|07112022|14:15:03|1411
2022|16112022|231108479433|Y|SANDEEP R
PATEL|1234567890|||N|N||18805.62||Y|National - 10000|0.00|||||||||||||||||SUSPECTED
FRAUD TRANSACTION|||||N|N||||
```

**Example:** Update record

F010161120221|CAN15112022000043446|Y|N|DEC|CAN|VISA|POS|OTH|||16112022|07112022|14:15:03|14112022|16112022|231108479433|Y|SANDEEP R PATEL|1234567890||N||N||18805.62||Y|National - 100000|0.00||||||||||||||||||SUSPECTED FRAUD TRANSACTION||||||N||N||||

**Annex**

**Payment Transaction Instrument**

Payment Transaction Instrument Code	Payment Transaction Instrument
BNK	Bank Account
PAI	Paper Instruments
DEC	Debit Cards (including tokenised debit card or virtual debit card)
CRC	Credit Cards (including tokenised credit card or virtual credit card)
PPI	Pre-paid Payment Instruments (wallet or physical card)
OTH	Other

**Payment System Category**

Payment System Code	Payment System Involved
ROP	RBI Operated Payment Systems (RTGS / NEFT)
NOP	NPCI Operated Payment Systems (IMPS, NACH, UPI, BBPS, NETC, CTS, AEPS, BHIM Aadhaar Pay)
CAN	Card Networks (VISA, Mastercard, Rupay, Diners, Amex)
ATM	ATM Networks
PPI	Prepaid Payment Instrument Issuers
CMO	Cross-Border Money Transfer Operators
TRD	Trade Receivables Discounting System (TReDS)
IMO	Instant Money Transfer Operators
INB	Intra-Bank (Banks' Core Banking System)
OTH	Other

Payment System Involved : Payment System Involved	Name of Payment System	Payment System Code
Based on input in 3C – Payment system category, the name of payment system used – RBI operated payment systems	Real Time Gross Settlement	RTGS
	National Electronic Funds Transfer	NEFT

NPCI Operated Payment Systems	Immediate Payment Service	IMPS
	National Automated Clearing House	NACH
	Unified Payments Interface	UPI
	Bharat Bill Payment System	BBPS
	National Electronic Toll Collection	NETC
	Cheque Truncation System	CTS
	Aadhaar enabled Payment System	AEPS
	BHIM Aadhaar Pay	BHIMAP
Card Networks (Visa, Mastercard, Rupay, Diners, Amex)	American Express Banking Corp., USA	AMEX
	Diners Club International Ltd., USA	DINERS
	MasterCard Asia / Pacific Pte. Ltd., Singapore	MASTER
	National Payments Corporation of India (RuPay)	NPCI
	Visa Worldwide Pte. Limited, Singapore	VISA
ATM Networks (list of authorised ATM networks);	Bank of India	BOIATM
	Euronet Services India Private Limited	EURATM
	National Payments Corporation of India (NFS)	NFSATM
	Punjab National Bank	PNBATM
	State Bank of India	SBIATM
	Other – On Us Transaction	ONUS
Prepaid Payment Instrument Issuers	Prepaid Payment Instrument Issuers – Not Applicable	PPI-NA
Cross-Border Money Transfer Operators (list of authorised MTSS Principals);	Bahrain Financing Company, BSC (C)	BFCBSC
	Continental Exchange Solutions Inc, USA	CESUSA
	Fast Encash Money Transfer Services Ltd.	FEMTSL
	Mastercard Transaction Services (Canada) Inc.(formerly Transfast Inc., Canada and Global Foreign Exchange Inc.)	TICCAN
	MoneyGram Payment Systems Inc, USA.	MGPUSA
	Muthoot Finserve USA Inc. {formerly Royal Exchange (USA) Inc.}	MUTUSA
	UAE Exchange Centre LLC, UAE	UAEECL
	Wall Street Exchange Centre LLC, UAE	WSEUAE
	Western Union Financial Services Incorporated, USA	WUFUSA
TReDS (list of authorised TReDS entities);	A.TREDS Limited	ATREDS

	Mynd Solutions Private Limited	MTREDS
	Receivables Exchange of India Limited (RXIL)	RTREADS
Instant Money Transfer Operators – Not Applicable;	Instant Money Transfer Operators – Not Applicable;	IMTP-NA
Intra-Bank – Not Applicable;	Intra-Bank – Not Applicable;	INTRA-NA
Others – Not Applicable;	Others – Not Applicable;	OTH-NA

**Payment Channel Used**

<b>Payment Channel Code</b>	<b>Payment Channel Used</b>
BRN	Branch
INT	Internet (Online)
MBL	Mobile
ITB	Internet Banking
MOB	Mobile Banking
ATM	ATM
POS	POS
BCA	BC Agent
IVR	IVR
MOT	MOTO
OTH	Others

**Nature of Fraud**

<b>Fraud Nature Code</b>	<b>Nature of Fraud</b>
ACH	Account Hacking / Compromise / Identity theft
PHH	Phishing
RMD	Remote Capture of Device
LSI	Lost / Stolen Device / Instrument
CRS	Card Skimming
VIS	Vishing
SMI	Smishing
SIS	SIM Swap
WBC	Website Cloning / Fraudulent Link
FRA	Fraudulent App
EHC	Email Hacking / Compromise
FMP	Forgery / Modification of Payment
MRC	Merchant Collusion
CLR	Collect Payment Request
OTH	Other