Indian Cyber Crime Coordination Centre

CYBER DOST

Citizen Financial Cyber Fraud Reporting & Management System

Helpline No 1930

Citizen Financial Fraud Reporting and Management System.

Helpline No: ✆1930

F A Q

General FAQ

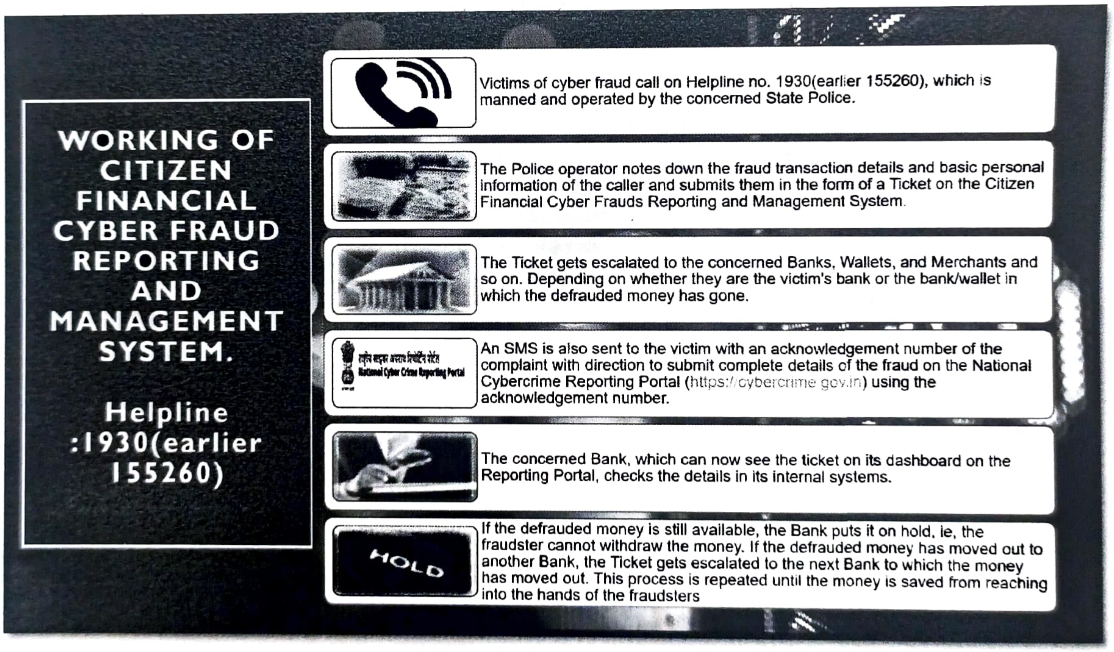
1. What is Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)?

The Citizen Financial Cyber Fraud Reporting and Management System has been developed by the Indian Cyber Crime Coordination Centre and is operated by respective State/UT which brings together Law Enforcement Agencies of States/UTs, Banks and Financial Intermediaries on a single platform to take immediate action on the complaints regarding financial cyber frauds received through helpline number 1930. The calls are being received by respective State/UT police officials.

I4C, MHA is the platform provider. Complaints are lodged and handled by respective State Law Enforcement Agencies.

2. How does the Citizen Financial Cyber Fraud Reporting and Management System operate?

Flow of the Fraud reporting system is briefed in the info graphic below:


राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
HOLD

WORKING OF CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM.

Helpline :1930(earlier 155260)

Victims of cyber fraud call on Helpline no. 1930(earlier 155260), which is manned and operated by the concerned State Police.

The Police operator notes down the fraud transaction details and basic personal information of the caller and submits them in the form of a Ticket on the Citizen Financial Cyber Frauds Reporting and Management System.

The Ticket gets escalated to the concerned Banks, Wallets, and Merchants and so on. Depending on whether they are the victim's bank or the bank/wallet in which the defrauded money has gone.

An SMS is also sent to the victim with an acknowledgement number of the complaint with direction to submit complete details of the fraud on the National Cybercrime Reporting Portal (https://cybercrime.gov.in) using the acknowledgement number.

The concerned Bank, which can now see the ticket on its dashboard on the Reporting Portal, checks the details in its internal systems.

If the defrauded money is still available, the Bank puts it on hold, ie, the fraudster cannot withdraw the money. If the defrauded money has moved out to another Bank, the Ticket gets escalated to the next Bank to which the money has moved out. This process is repeated until the money is saved from reaching into the hands of the fraudsters

3. Is there an official link or launch information from the Government?

A press release has been given by MHA

https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1727990

4. Who are the existing participants of the Citizen Financial Cyber Fraud Reporting and Management System arrangement?

State/UTs Law Enforcement Agencies, Major Banks, Small Finance Banks, Payments Banks, Wallets, E-Commerce companies, Payment Gateways are part of the arrangement.

(List is attached in Appendix 1 as on 03.03.2022)

5. Who manages the helpline number and complaints reported through the help line number?

Respective State/UT Law Enforcement Agencies manage the help line number and officials designated by the respective State/UT Law Enforcement Agency receive calls from complainants and enter the required details on their behalf. Complaints are registered through the helpline number and also through the portal.

6. How can citizens register complaint on the Citizen Financial Cyber Fraud Reporting and Management System?

Citizens can register their complaints through the helpline number 1930. Complainants can call on the helpline number 1930 and provide few mandatory details like Name, Mobile Number, Address, Transaction details etc. and after receiving acknowledgement number need to make a formal complaint on the portal (https://cybercrime.gov.in/) within 24 hrs using the acknowledgement number received on SMS.

7. Whether the complainant has to register a formal complaint at Police Station also?

No, Complainant has to register formal complaints on the National Cybercrime Reporting Portal (https://cybercrime.gov.in) within 24 hrs after registration of complaints through the helpline number using the link and acknowledgement number sent to them through SMS.The complaint is automatically forwarded to the concerned police station.

FAQ for Financial Intermediaries – Banks, Payment Gateway-Aggregators

8. How can an intermediary join/apply for access to the Citizen Financial Cyber Fraud Reporting and Management System?

Any financial intermediary can get onboarded to the portal by sending a request mail to the Indian Cyber Crime Coordination Centre on i4c.finmod@mha.gov.in . Post verification, Login credentials for the portal will be created and sent by the I4C team. The Financial intermediary needs to appoint a nodal officer for the portal and send his/her details i.e. Name, Designation, Official Email & Mobile Number(For OTPs).

9. What if there is any update in the portal in terms of layout or content?

There is an option of “What’s new” in the portal where stakeholders can see details of any modifications to the portal.

10. We received a notification regarding fraud. What to do?

- Banks may use the UTR/Transaction number present in the complaint to identify the fraud transaction from their banking system.
- If fraudulent money is present in the account, the amount could be marked as Lien.

- If funds have been transferred to other accounts, details could be given thereof under the tab 'Money transferred to'.
- If funds are withdrawn, details of the same could be entered against the complaint like ATM details, AEPS details, POS ID etc.

11. What should you reply to customers asking the reason for putting a reported fraud money at Lien?

Banker can reply, "A complaint has been received from the respective state police involving your account".

12. How to defreeze the account, if a complaint has been withdrawn due to a false complaint/resolution?

Banks may receive a direction from the concerned State Police who have registered the complaint to defreeze the account.

13. How to initiate the refund procedure of the Lien Amount?

Banks have their internal procedure to refund/release the Lien amount. There are many options to initiate refund, like direct refund (based on internal investigation), court order based refund initiation, police communication based refund initiation, etc.

14. What must be put on hold – the fraud amount or the whole bank account?

It is recommended to mark the fraud amount as a lien. However, it is at the sole discretion of the Bank/investigating officer to freeze the whole account in case of suspicion.

15. What is the use of the "others" option given while taking action on the complaint?

The "others" option must be used to mention the name of the bank/wallet/merchant which are not listed on the portal through which the fraud amount has been transferred/utilized.

16. What to do if the details in the complaint are missing or wrongly entered?

The nodal officer may reassign it to the previous intermediary to correct the data and send it back to the concerned financial intermediary.

17. How to contact the nodal officer who has registered the complaint on the portal?

Click the nodal officer tab in the navigation menu to view the details of nodal officers.

18. **If the amount is withdrawn through ATM, AEPS OR POS, what needs to be done?**

The ID of the ATM, AEPS or POS along with the withdrawal amount and location must be entered in the prescribed tab.

19. **Can contact details of nodal officers be shared with the complainant?**

No, contact details of Bank/Intermediaries holding amount or I4C officials must not be shared with the complainant. Only details of concerned State/UT police may be shared, if required.

20. **Whether the Complaint getting reported on Cyber Crime Reporting Portal needs to be treated as a Registered Police complaint filed by complainant/ customer?**

Yes, if it has been reported through the National Cybercrime Reporting Portal.

21. **Whether the Bank can block / withhold the funds on the basis of the complaint's acknowledgement number that gets reported on the helpline number or NCRP?**

Yes, Bank/intermediaries can put the disputed amount on lien on the basis of the complaint's acknowledgement number so that amount can be refunded later, after investigation of the complaint by concerned State/UTs LEAs.

22. **How should complaints belonging to a Merchant on a Payment Gateway or an Aggregator be handled?**

PA-PG may put a lien on the reported fraud amount of the merchant's virtual account and consequently hold the settlement of the disputed amount upon request by LEAs.

FAQ for Ecommerce Companies

23. **How to join/apply for access to Citizen Financial Cyber Fraud Reporting and Management System?**

Any Ecommerce Company can get onboarded on the portal by sending a mail request to Indian Cyber Crime Coordination Centre at i4c.finmod@mha.gov.in. Post verification, Login credentials for the portal will be created by the I4C team. The **Ecommerce Company** needs to appoint a nodal officer for the portal and send his/her details i.e. Name, Designation, Official email & Mobile Number (For OTPs).

24. **What if there is any update in the portal in terms of layout or content?**

There is an option of "What's new" in the portal where stakeholders can see details of any modifications to the portal.

25. **What to do if fraudulent money is used on an E-Commerce Site?**

The E-Commerce Company may do a due diligence on the fraud complaint received and hold the delivery of the product that was purchased using fraud money and refund money as per applicable policy.

26. **What if a coupon was used to conduct fraud on the website? What should be done?**

Orders pertaining to the coupon should be tracked and put on hold.

FAQ for State Police

1. **What information needs to be entered at the time of receiving a complaint?**

All the fields marked as mandatory with the use of asterisk (*) sign, needs to be filled in correctly. In addition to this, if there is any information that you think is necessary to carry out an investigation, must also be mentioned accurately. Additional details of the incident may be mentioned in the 'incident description'.

2. **Is checking the information before submission necessary?**

Yes, it is necessary to check the information/data provided by the complainant for any missing or incomplete information. This can be checked using the 'save and preview' tab.

3. **What is the use of the "others" option given while taking action on the complaint?**

The "others" option must be used to mention the name of the bank/wallet/merchant which are not listed on the portal through which the fraud amount has been transferred/utilized.

4. **Can the contact details of nodal officers be shared with the complainant?**

No, contact details of Bank/Intermediaries holding amount or I4C officials must not be shared with the complainant. Only details of concerned State/UT police may be shared, if required.

5. **Is there any editing option given in case of any mistakes committed while filling the information?**

No, there is no edit option provided on the portal. However, before submitting the complaint, a tab of "save and preview" is given to double check the details of the complaint and its completeness.

6. **What is the maximum time frame of reporting the fraudulent transactions through the Helpline number 1930?**

It is recommended to report the complaints within 48 hrs. However, if the fraudulent amount is huge and needs immediate action, the officer may report older complaints as well.

Appendix 1

S No.	Bank				
1	Union Bank of India(including Andhra Bank and Corporation Bank)	29	Karnataka Bank Ltd	57	Meghalaya Rural Bank
2	State Bank of India	30	Federal Bank	58	HP Gramin Bank
3	Paytm Payment Bank	31	IndusInd Bank	59	Puduvai Bharathiar Grama
4	RBL Bank	32	Equitas Bank	60	Vidharbha Konkan Gramin Bank
5	Jammu and Kashmir Bank	33	DCB Bank (Development Credit Bank)	61	Kerala Gramin Bank
6	HDFC Bank	34	State Bank of India (Credit card)	62	Punjab & Sind Bank
7	Bank of Baroda (Including Vijaya Bank and Dena Bank)	35	Airtel Payments Bank	63	Andhra Pragathi Grameena Bank
8	Indian Overseas Bank	36	Andhra Pradesh Grameena Vikas Bank	**S No.**	**Merchant**
9	Karnataka Gramin Bank	37	Indian Bank (including Allahabad Bank)	1	CRED
10	Jio Payments Bank Ltd	38	Telangana Grameena Bank	2	Bharat Pe
11	State Bank Of Mauritius	39	Central Bank of India	3	ATOM
12	IDFC First Bank	40	Bank of India	4	Cashfree
13	Axis Bank	41	Kotak Mahindra Bank	5	Flipkart
14	South Indian Bank	42	Punjab National Bank (including Oriental Bank of Commerce and United Bank of India)	6	Billdesk
15	Standard and Charted Bank	43	Bandhan Bank	7	Khata Book
16	ICICI Bank	44	Bank of Maharashtra	8	Nobroker Technologies Solution Private Ltd
17	India Post Payments Bank	45	Tamilnad Mercantile Bank Ltd.	9	ShopClues
18	Yes Bank	46	Ujjivan Small Finance Bank Ltd	10	Snapdeal
19	DBS Bank (Including Lakshmi Vilas Bank)	47	IDBI Bank	11	Croma
20	Citi Bank	48	AU Bank	**S No.**	**Wallet**
21	UCO Bank	49	Canara Bank (including Syndicate Bank)	1	Razorpay
22	Fino Payments Bank	50	Suryoday Bank	2	Payu
23	City Union Bank	51	NSDL Payments Bank Ltd	3	PhonePe
24	ESAF Small Finance Bank	52	Baroda U.P. Bank	4	Mobikwik
25	Karur Vysya Bank	53	GSC Bank	5	Freecharge
26	Chhattisgarh Gramin Bank	54	Dhanlaxmi Bank	6	Dhani Pay
27	Tamil Nadu Grama Bank	55	Catholic Syrian Bank	7	Ease Buzz
28	Baroda Gujarat Gramin Bank	56	Nainital Bank	8	Amazon Pay