A BANKBAZAAR PRIMER
JUNE 2024

SECURE PAYMENTS

A GUIDE TO TRANSACTING SAFELY

FOREWORD

Financial fraud is an ever-evolving threat that you, or someone you know, has likely been a victim of. This threat extends to banks and financial institutions dealing with customers' financial data. With AI, financial frauds are becoming highly sophisticated, and often hard to detect.

The Indian Cybercrime Coordination Centre (I4C) reported that over the last three years, digital financial frauds have led to staggering losses worth ₹1.25 lakh crore.

In 2023 alone, over 13,000 cases of financial fraud were recorded, nearly half of which were digital payment fraud (card/internet).

According to data from the National Cybercrime Reporting Portal (NCRP), victims of digital financial fraud reported to have lost at least ₹10,319 crore.

The rising popularity of digital payment methods, including credit cards, has led to an uptick in digital financial fraud. Staying vigilant and aware has, thus, become essential. This primer covers various types of fraud and the warning signs to watch out for. Also included are practical fraud-prevention strategies you can use to protect your finances and a glimpse into the Reserve Bank of India's rules on credit card fraud prevention that you will find useful.

UNDERSTANDING FINANCIAL FRAUD

Types of financial fraud & how to recognise them

Type of fraud	How it's done	Identifying signs
Phishing	Fraudsters send fake emails or messages pretending to be from banks or payment apps to steal information	• Emails/SMS asking for personal details or OTP • Links directing to fake websites • Unusual grammar or spelling errors
SIM Swapping	Fraudsters duplicate your SIM card to intercept OTPs and complete transactions, including those from your credit card	• Sudden loss of mobile network • Unable to make or receive calls • Unusual activity in your bank account
Card Skimming	Devices are installed at ATMs or POS terminals to capture card details during transactions	• Unusual attachments on ATMs or POS terminals • Unauthorized transactions on your bank statement
Vishing (Voice Phishing)	Fraudsters call pretending to be bank officials to extract confidential information	• Calls asking for personal or banking details • Callers creating a sense of urgency or fear
Fraudulent UPI Requests	Fraudsters send fake UPI payment requests, tricking victims into approving them	• Unexpected UPI payment requests • Requests from unknown contacts
Overpayment Scams	Fraudsters send a small amount and ask for a larger amount back, claiming an error	• Receiving small payments from unknown sources • Requests to return a larger amount than received
Fake Customer Service Numbers	Fraudsters post fake customer service numbers online, leading victims to share sensitive personal or banking information	• Unverified customer service numbers online • Request for personal or banking details during the call

FINANCIAL FRAUD STATISTICS

Type of Fraud	Rise in cases/amount	Source
Total financial fraud cases	1.13 million cases in 2023	Lok Sabha reply
Digital payment fraud (Card/Internet)	6,659 cases in 2023	RBI
Amount involved in financial cyber fraud	₹7,488.6 crore in 2023	Lok Sabha reply
Financial fraud complaints	4.7 lakh complaints (saved ₹1,200 crore)	Indian Cyber Crime Coordination Centre
Total financial frauds	Increased 65% in 2022	Finance Ministry (Hindu Business Line)
ATM & other financial frauds	• Grew 88.8% in value between 2021-2022 • ₹1,119 crore in 2021 (1.08 million cases) • ₹2,113 crore in 2022 (1.78 million cases)	Finance Ministry (Hindu Business Line)
UPI-related scams	Account for 55% of total digital payments fraud	NPCI
Customers affected by cyber fraud	2000 customers affected monthly	NPCI

IMPACT OF FINANCIAL FRAUD

Financial fraud severely impacts personal finances, causing direct monetary losses and significant stress. Victims face drained accounts, unauthorized transactions, damaged credit scores, and a loss of trust in financial institutions. The emotional toll includes anxiety and distrust, lasting well beyond the resolution of the fraud. This disruption not only affects the individual's financial stability but also erodes confidence in digital banking services, altering how people manage their finances.

CASE STUDY #1

Man clicks unverified link, loses ₹60,000

What happened

A senior citizen who lived with her son received a call from someone allegedly calling on behalf of Maharashtra Natural Gas Limited, a gas provider supplying piped gas to homes in Maharashtra. The caller, feigning urgency, informed the lady of a pending gas bill, which, if not paid immediately would result in their connection being disconnected. The lady, in a rush and hassled by this information, hurriedly handed the phone to her son to sort out that matter.

The caller reiterated the urgency of the pending gas bill payment and asked the son to pay via a specific link that he, the caller, would share. The son proposed making a ₹100 test payment to which the caller agreed. The link, once opened, displayed the details of the gas connection, such as the account ID, the person in whose name it was registered, etc. Believing the link to be genuine, the son entered his card details to make the test payment of ₹100 but ended up losing ₹60,000.

What not to do

- If contacted by an unverified person for outstanding payments, always contact the organisation itself to confirm the status of the payment.
- Never click on any unverified links received via email, direct message, or SMS, especially ones demanding urgent payment or even rewards. These may usually be sent from a mobile number. Meanwhile, banks usually send bulk messages with set prefixes like AD, BZ, BX, VK, etc., that indicate the sender's origin and type of message.
- Never enter your credit card details on unverified websites or links.
- Always check for the 'HTTPS' prefix in a website's URL to verify that it is secure.
- If you have clicked on a link accidentally, do not enter any sensitive financial information on the page. Always make bill payments via the service provider's official website.

Customer's Liability

In this case, the financial loss happened due to the son's negligence after he shared the payment credentials on an unverified website.

In such a situation, only a limited liability policy may be applicable. The customer may have to bear the full monetary loss until they report the incident to the bank or concerned authority. Any loss incurred after the transaction was reported to the bank shall be borne by the bank.

CASE STUDY #2

Lady loses 60k after swiping her credit card at a local market

What happened

A lady from Jaipur went to a local market in Bangalore to purchase a few items from a small independent shop. To make the payment, the shopkeeper used a credit card machine on which the lady entered her credit card PIN. The payment went through smoothly and she returned home.

A few hours later, the lady received a transaction alert for her credit card with a charge of ₹50. Since it was close to bedtime and the amount was small, she didn't think much of it. Soon after, she received a call from her bank about a potential fraudulent transaction. Suspecting it to be a scam call, she hung up. The next morning though, a nastier surprise awaited, for she received yet another transaction alert for her credit card, but this time for ₹20,000. That's when the severity of the situation sunk in and she immediately reported the unauthorised transaction to the bank and got her card blocked.

This incident is potentially a case of card skimming done using a rigged card payment machine with the card PIN being possibly traced or recorded by the machine or the POS terminal attendant. Fortunately, she flagged these transactions within 24 hours of the incident and was able to recover her funds.

What not to do

- When shopping at a market where payment security is uncertain, refrain from using a debit card or use your credit card. Credit card disputes are easier to initiate, and transactions are easier to reverse. Moreover, you do not lose money from your bank account.
- Never ignore any transaction alerts, no matter how small the transaction amount. These can help you keep track of your card activity.
- Banks typically monitor your card transactions and will contact you if they suspect an unauthorised activity on your card. Attend calls from your bank carefully and patiently before responding.
- If you see signs of tampering on the card machine or suspect it may be compromised, cancel your transaction.

Customer's Liability

There was no negligence on the customer's part, but a third-party breach, which led to this incident.

Because the customer alerted the bank and got their card blocked within 24 hours of the incident, they were eligible for zero liability.

However, the customer did have to pay a certain fee to obtain the replacement card.

CASE STUDY #3

Bank SMS Screenshot Scam

What happened

In May 2024, a woman from Bangalore received a call from a person pretending he needed help to transfer money to her father. He claimed having issues with his bank account and asked the woman to receive the funds on her father's behalf. Moments later, the lady received two SMS alerts identical to her bank's notifications, indicating the credited amounts. Upon receiving the SMS, the man called her again claiming he had accidentally transferred ₹30,000 instead of ₹3,000, and urged her to return the excess which he needed to pay an urgent medical bill.

Thanks to the woman's awareness, she noticed the discrepancies in the SMS and also checked her bank account for any credit. There was none. Convinced that it was a scam, she stopped responding to the man's plea for money. Exploiting urgency and faking familial connections are just two of the many ways fraudsters trick people into parting with their money.

What not to do

- Never act on urgent financial requests from unknown sources. Always verify such requests before taking appropriate action.
- Never respond or interact with messages, emails, or links received from unofficial sources.
- Always check such messages for discrepancies, and confirm the same with your bank.
- If you are being solicited to provide urgent financial assistance to or by a family member, always confirm with the family member first. Voice-modulation software has also enabled a wave of scams where strangers sound like a family members making urgent pleas for money.

Customer's Liability

This incident is a good example of the customer's quick and careful thinking. They patiently processed the situation and were able to spot red flags in the SMS sent by the unidentified caller and did not act on their demand. Thus, no monetary loss occurred during this incident.

In case the woman had transferred the amount, the issuer would not have any liability and no restitution may have been possible in this case.

CASE STUDY #4

Bangalore resident's card gets skimmed, charged in the US

What happened

In 2023, a Bangalore resident received multiple notifications of their credit card being used in a funeral home in Florida, US, despite never having visited or carried out any transactions in the US. No OTP was requested for these transactions, indicating there was a potential breach of security measures typically deployed for credit card transactions in India. The transactions, totaling several hundred dollars, alerted the victim to potential fraudulent activity. He immediately reported the unauthorized charges and got the card blocked. The prompt reporting of the incident helped the man recover the lost funds.

What not to do

- Block your cards as soon as possible to prevent further misuse.
- Never ignore transaction alerts. Reach out to your bank immediately if you suspect unauthorised use.
- Keep your card details with utmost safety. Never enter sensitive financial information online except on trusted websites which have a robust security mechanism.

Customer's Liability

This incident is a an example of a potential data breach which led to the customer's credit card details being compromised and falling into the wrong hands.

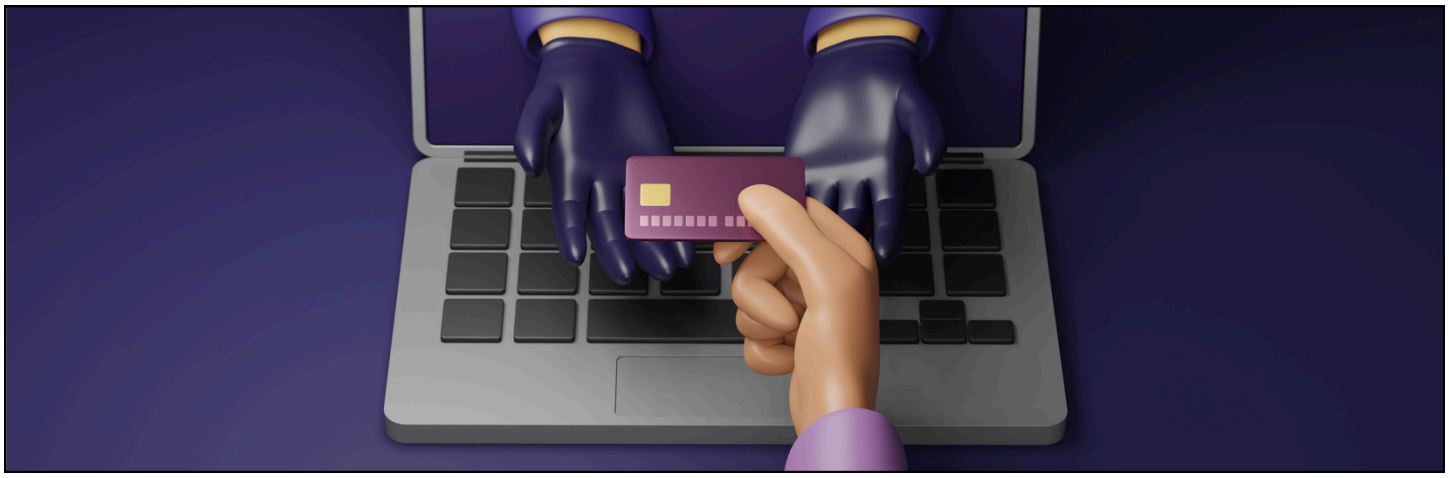
There was no negligence on the customer's part, and they lost no time in reporting the incident to their bank and blocking their card.

As a result, the customer was eligible for the Zero Liability policy offered by their bank and recovered the lost amount.

WHAT TO DO IF YOU LOSE MONEY

- **Report the incident immediately**: Promptly report the fraudulent incident to your bank or UPI app provider. Here, time is of the essence - the earlier you report, the higher will be your chances of being eligible for zero eligibility protection, subject to conditions.
- **Block your cards:** Request the bank to freeze your account and block your card to prevent further misuse.
- **Provide relevant detail**s: When reporting the incident to the bank, provide all information such as emails, SMSs, screenshots, transaction details, or any other incident-related details, if necessary. This documentation can help support your case.
- **Dispute resolution:** After filing the report, follow up on the dispute resolution process. Adhere to the reporting deadline and provide all necessary documentation to maximize chances of recovering your funds.
- **File a police report:** If required, file a complaint with the local cybercrime unit or police which can serve as an official record and may be necessary for further investigations.
- **Notify your credit bureau**: Don't forget to notify your credit bureau of the fraudulent incident to prevent it from impacting your credit score.
- **Monitor your accounts:** Check your credit card accounts regularly to track your transaction activity. This will allow you to flag and report suspicious without delay.

DOCUMENTS YOU'LL NEED



FRAUD ORIGINATING WITHIN INDIA

To report a fraudulent incident or transaction, you must provide the following documents based on whether the fraud is a domestic or international transaction. Remember, once your card has been blocked, it cannot be used again. The bank will issue you a new replacement card with a different number. However, your blocked card's account will remain active.

Domestic transactions

- Cardholder Dispute Form (CDF) with transaction details and signed by you.
- Incident Letter with the date and your signature, addressed to your bank. It must contain details about (a) Account number, card number, and date of loss, (b) Who had the card when the fraud happened and how you found out about the transaction, and (c) Any additional information about the fraud.
- Original FIR / Online FIR / Incident Letter with the police acceptance stamp. If the fraudulent transaction is equal to or above ₹20,000, it is mandatory to provide details of the card and transaction

FRAUD ORIGINATING ABROAD

In the case of a fraudulent international transaction, you must submit the following documents, in addition to a filled-in Customer Dispute Form and Incident Letter:

- FIR from the overseas local police is mandatory if the fraud involves an international transaction and the customer is in the location of the fraud.
- FIR is not required if the fraud involves an international transaction while the customer is in India.
- Passport copy including blank pages is mandatory for fraudulent international transactions and transactions where geographical location is unclear. In the absence of a passport, a signed declaration by the customer confirming that they do not hold a passport & were not in the city of fraud must be obtained.

In credit card fraud cases, the customer's liability depends on how quickly the card has been blocked after the fraud is discovered.

LIABILITY CONSIDERATIONS

Banks and credit card issuers usually have policies in place for fraud liability. Reporting the fraud promptly can often reduce your liability and increase the chances of reversing the transaction. The Reserve Bank of India has set guidelines that outline a customer's liability in the event of a fraud.

Card Blocking	Customer Liability
Blocked within 3 days from the date of the fraud	Zero liability
Blocked between 4 to 7 days from the date of fraud	• ₹10,000 (Credit cards with a limit up to ₹5 lakh) • ₹25,000 (Credit cards with a limit above ₹5 lakh)
Blocked after 7 days from the date of fraud	As per the bank's board-approved policy

Exceptions to the Zero Liability Policy
The Zero Liability policy is designed to help protect cardholders from fraudulent or unauthorised transactions. However, there are certain situations where cardholders may not qualify for such protection.

- **Delayed reporting**: Failure to report the unauthorized transaction to the bank within the set deadline may result in partial or full liability.
- **Cardholder's negligence**: Cardholders may be held liable for the loss incurred if they fail to adequately protect their account details and unintentionally share their card PIN, OTP, or any other sensitive financial information to facilitate the fraud.
- **Third-party usage**: Cardholders may also violate the terms of their card's use by handing over their card to a third party, which could be even a family member, colleague, or friend. Cardholders will bear any liabilities arising from such transactions.
- **Business/corporate, and prepaid cards**: Non-consumer cards like business/corporate cards, and prepaid cards are typically covered under a different liability policy than consumer cards and hence may not be covered under the Zero Liability policy.

WHAT THE RESERVE BANK OF INDIA SAYS

The Reserve Bank of India (Credit Card and Debit Card – Issuance and Conduct) Directions were issued in 2022 to emphasise the responsibility of banks and financial institutions in implementing effective safeguards to protect customers' interests. This includes establishing a framework for addressing customer complaints related to unauthorized transactions, outlining liabilities for both customers and institutions, and enforcing customer protection measures such as zero liability in certain cases and timely grievance redressal. In credit card fraud cases, the customer's liability depends on how quickly the card has been blocked after the fraud is discovered.

Here's what the master direction says on frauds and disputed payments.

5. Governance Framework
(b) Card-issuers shall put in place a mechanism for review of their credit card operations on half-yearly basis by the Audit Committee of the Board of Directors. The review shall include, inter-alia, customer service, frauds, complaints and grievance redressal, card usage analysis including cards not used for long durations and the inherent risks therein.

6. Issue of Credit Cards
iii. Card-issuers may consider introducing, at the option of the customers, an insurance cover to take care of the liabilities arising out of lost cards, card frauds, etc. In cases where the card-issuers are offering any insurance cover to their cardholders, in tie-up with insurance companies, the card-issuers shall obtain explicit consent in writing or in digital mode from the cardholders along with the details of nominee/s.

10. Billing
(d) No charges shall be levied on transactions disputed as 'fraud' by the cardholder until the dispute is resolved.

12. Reporting to Credit Information Companies
(b) Before reporting default status of a credit cardholder to a Credit Information Company (CIC), the card-issuers shall ensure that they adhere to the procedure, approved by their Board, and intimate the cardholder prior to reporting of the status. In the event the cardholder settles his/her dues after having been reported as defaulter, the card-issuer shall update the status with CIC within 30 days from the date of settlement. Card-issuers shall be particularly careful in the case of cards where there are pending disputes. The disclosure/release of information, particularly about the default, shall be made only after the dispute is settled. In all cases, a well laid down procedure shall be transparently followed and be made a part of MITC.

26. Redressal of grievances
(a) Card-issuers shall put in place a Grievance Redressal Mechanism within the card issuing entity and give wide publicity about it through electronic and print media. The name, direct contact number, email-id and postal address of the designated grievance redressal officer of the card-issuer shall be mentioned on the credit card bills and account statements. The designated officer shall ensure that grievances of cardholders are redressed promptly without any delay. Specific timelines may be stipulated in the Board approved policy for issuance of cards, redressal of grievances and compensation framework. The grievance redressal procedure and the Board approved policy shall be displayed on the website of the card-issuer with a clearly visible link on the homepage

(b) Card-issuers shall ensure that their call centre staff are trained adequately to competently handle and escalate, a complaint, if necessary. The Grievance Redressal process shall have a provision for automatic escalation of unresolved complaints from a call center/base level to higher authorities. There shall be a system of acknowledging customers' complaints for follow up, such as complaint number/docket number, even if the complaints are received over phone.

(c) Card-issuers shall be liable to compensate the complainant for the loss of his/her time, expenses, financial loss as well as for the harassment and mental anguish suffered by him/her for the fault of the card-issuer and where the grievance has not been redressed in time. If a complainant does not get satisfactory response from the card-issuer within a maximum period of 30 days from the date of lodging the complaint, he/she will have the option to approach the Office of the RBI Ombudsman under Integrated Ombudsman Scheme for redressal of his/her grievance/s.

BEST PRACTICES FOR FRAUD PREVENTION

- **Set transaction limits** - As a first line of defence, make use of your credit card's built-in controls to limit where and how your card can be used, i.e., online, point of sale terminals, or via tap & pay. You may also set transaction limits different types of transactions to limit your liability in case of unauthorised use of your card. Check if you can tweak these settings for domestic and international transactions.
- **Never share sensitive information** – Sensitive data like credit card details, PINs, and login passwords must never be shared with anyone. Also refrain from sharing personal information online. Avoid using public Wi-Fi or entering sensitive banking information over unsecured public networks.
- **Set up transaction alerts & review credit card statements**– Transaction alerts, for primary and add-on cards will help you keep tab on what the card is being used for. Review your credit card and bank statements frequently to check for unauthorized transactions.
- **Never leave your card unattended** – When making payments at restaurants or fuel stations, always keep your card within sight when handing it over to the attendant. Use EMV chip cards to reduce the risk of skimming and inform the staff promptly if you notice anything unusual with the card slot or Point of Sale device.
- **Shop online safely** – Only shop from trusted and established websites that offer secure payment gateways. Enable Two-Factor Authentication (2FA) for your accounts for added security.
- **Update devices regularly** – Security patches and updates are typically offered by the device manufacturers and software developers to help device owners stay protected against the latest cyber security threats.
- **Be vigilant** – Acquaint yourself with the warning signs of online scams. These could be suspicious emails/SMSs/websites, unsolicited payment requests, suspicious links, or request for banking information, among other things. If fraudulent activity occurs, promptly report it to your bank.

THE C.H.E.C.K. LIST

Vigilance is key to avoiding fraud. In suspicious situations, ask yourself these questions to determine the best course of action.

Credibility	**Is this payee trustworthy?** Have you verified the authenticity of the business or individual requesting a credit card payment?
Haste	**Does this request seem urgent or too good to be true?** Is there an unusual sense of urgency or an offer that seems unbelievably good?
Excess Information	**Am I being asked for too much personal information?** Are you being asked for sensitive information like your full card number, CVV, PIN, or passwords?
Control	**Have I initiated this transaction?** Is this transaction or request something you initiated, or did it come unsolicited?
Known Platform	**Is this transaction happening on a secure platform?** Are you using a secure and reputable website, a secure payment gateway, a known POS machine or ATM?

IN SUMMARY

There have been several forward-thinking initiatives in the BFSI space by the previous governments and the RBI. To build on this momentum, it is essential to maintain and enhance these efforts. Long-term planning and visionary changes, such as creating a digital public good for credit reporting, inclusive of a national fraud registry with daily updates, will strengthen national cybersecurity and fraud prevention and increase costumer confidence in not just digital payments but in the BFSI ecosystem on the whole.

Author
Malvika Singhal
Manager, Communications
malvika.singhal@bankbazaar.com

Editor
AR Hemant
AVP, Communications
arhemant@bankbazaar.com

Nanda Padmanabhan
DGM, Communications
nanda.padmanabhan@bankbazaar.com

About Us
BankBazaar.com is India's largest fintech co-branded credit card issuer and online platform for free credit score. It has a base of 60 million registered users who use the platform for free credit score tracking and in-depth personal finance content and comparison tools.

Its range of co-branded credit cards with India's leading banks is driving the platform's rapid growth with more than half its customers now opting for BankBazaar's own co-branded products. The company is on track to facilitate one million active BankBazaar co-branded credit cards in force.

Supported by global investors such as Experian, Eight Roads, Peak XV Partners, WSV, and Amazon, BankBazaar has been at the forefront of democratising finance by providing Indians with frictionless access to credit.

The company exited FY2024 with an audited revenue ₹215 crore, growing 36% year-on-year.

Adhil Shetty, CEO, BankBazaar.com, said: "BankBazaar has been focussed on three things: great technology, customer focus, and the bottom-line. I am proud to say that we are one of the few fintechs in the world to be growing rapidly and profitably.

BankBazaar is well positioned to accelerate this revenue growth rate further in FY25 while targeting full year EBITDA profitability. This strategy for profitable and sustainable growth has been in the works for over three years. We've built a co-branded portfolio of digital products with proven customer traction, which has created sustainable revenue while improving margins."

bankbazaar
Credit To You