Beware of Fake Loan Apps: Protect Yourself from Digital Lending Fraud

Digital loan apps have made borrowing quick and convenient in India. However, fraudsters may create fake loan apps that look genuine but are designed to steal a customer's personal information, money, or both. A few simple checks can protect customers from **fake loan app fraud**.

How Do Fake Loan Apps Operate?

Fraudulent loan apps often attract customers through advertisements, SMS, WhatsApp messages, or social media posts. These advertisements may promise an **"instant loan", "guaranteed approval",** or **"loan without documents".**

These apps may:

- Falsely claim to be connected with an RBI-regulated bank or Non-Banking Financial Company, also called an NBFC.
- Approve a loan without properly checking the borrower's income, PAN, or credit history.
- Ask for unnecessary access to contacts, photographs, SMS, call logs, camera, microphone, or location.
- Use SMS sender names or logos that appear official.
- Ask customers to download an APK file through a link instead of using an official app store.
- Deduct unexpected charges or demand repayment within a very short period.
- Misuse personal data to threaten, harass, or shame customers.

Check Before Applying

Customers should not share PAN, Aadhaar, bank details, or OTPs without completing the following checks:

1. Verify the App and Lender

If an app claims to be connected with FincFriends, check the official List of LSPs and Digital Lending Apps. This page lists the digital lending apps and service providers officially associated with FincFriends.

Customers should also check RBI's public directory under **RBI website → Citizen's Corner → Digital Lending Apps**. This directory helps customers verify whether an app's claimed association with an RBI-regulated bank or NBFC has been reported by that entity.

2. Use Only Official App Stores

Download an app only from the Google Play Store or Apple App Store, using the link available on the lender's official website.

Never install an APK file received through SMS, WhatsApp, email, or social media.

Note: Availability on an app store alone does not prove that an app is genuine. Customers should always verify the lender and the app's official association.

3. Check the Permissions

A customer should not continue if an app demands unnecessary access to contacts, gallery, SMS, or call logs. The customer should read the app's privacy policy and understand why any personal information is being collected.

Know the Warning Signs

Stop immediately if an app or caller:

- Guarantees loan approval without document or credit checks.
- Demands an advance payment to "release" the loan.
- Asks for an OTP, UPI PIN, ATM PIN, password, or CVV.
- Pressures the customer to act or make a payment immediately.
- Asks the customer to transfer money to a personal bank account, mobile number, or unknown UPI ID.
- Refuses to provide the lender's full legal name, address, or grievance contact details.
- Does not provide a loan agreement or Key Facts Statement.

Borrow Safely

Before accepting a loan offer, the borrower should carefully read the **Key Facts Statement**, also called the KFS.

The KFS should clearly explain important information such as:

- Loan amount and repayment period
- Interest rate and Annual Percentage Rate, or APR
- Processing fee and other charges
- Penal charges for delayed payment

- Repayment amount and schedule
- Total cost of the loan
- Applicable cooling-off period

RBI requires regulated lenders to provide the KFS before the loan agreement is executed. The KFS should be written in simple language understood by the borrower.

The borrower should repay the loan only through the official in-app or bank channel stated in the loan documents. Payments should never be made to an unknown person, personal bank account, or unauthorised UPI ID. Also, customers should save receipts, transaction IDs, account statements, and screenshots of every payment.

What to Expect from FincFriends' Recovery Process

FincFriends and its authorised representatives will follow applicable laws and fair recovery practices. Recovery calls will be made only during permitted hours.

FincFriends and its authorised representatives will **not**:

- Threaten, abuse, or intimidate a customer.
- Publicly shame a customer.
- Send insulting or misleading messages.
- Contact the customer's friends, relatives, or colleagues to cause embarrassment.
- Misuse the customer's photographs, contacts, or personal information.
- Ask the customer to make a repayment through an unauthorised personal account.

Any conduct of this nature should be reported immediately through FincFriends' official grievance redressal channel.

How to Report a Suspicious Loan App

Customers should keep screenshots, app links, telephone numbers, messages, payment records, and bank transaction details as evidence. The matter can then be reported through the appropriate channel:

1. **FincFriends Grievance Redressal Officer:** Use the current contact details provided on the FincFriends website, app, KFS, or Grievance Redressal Policy.
2. **RBI Complaint Management System:** If a complaint against an RBI-regulated bank or NBFC is not resolved satisfactorily, visit https://cms.rbi.org.in.

3. **National Cyber Crime Reporting Portal:** Visit cybercrime.gov.in or call **1930** immediately if money has been lost in a financial cyber fraud.
4. **Sachet Portal:** Report a suspected unauthorised financial entity at sachet.rbi.org.in.
5. **FACE:** Report or seek support regarding a suspected fraudulent loan app at **sro@faceofindia.org**. FACE also advises customers to use verified lenders and avoid sharing information or making payments through unverified channels.

Stop. Check. Borrow Safely.

Never share an OTP, PIN, or password. Never install an app from an unknown link. Always verify the lender, read the KFS, and use only official payment channels.
