Flipkart Finance Private Limited

Fraud Prevention

General Principles of Fraud Prevention

- **Be Skeptical and Vigilant:** Always question unsolicited requests for personal or financial information, whether they come via phone, email, text message, or social media.
- **Educate Yourself:** Stay up-to-date on common scam tactics like phishing, vishing (voice phishing), smishing (SMS phishing), and different types of scams (e.g., investment, lottery, romance).
- **Your Bank Will Never Ask:** Remember that your bank will never ask you for sensitive information such as your full credit/debit card number, CVV, PIN, or OTP (One-Time Password) over the phone or via email.

Do's for Preventing Banking Fraud

Protecting Your Personal Information and Accounts

- **Use Strong and Unique Passwords:** Create complex passwords for your banking and online accounts. Use a combination of random letters, numbers, and special characters. Consider using a password manager to securely store them.
- **Enable Two-Factor or Multi-Factor Authentication (2FA/MFA):** This adds an extra layer of security. In addition to your password, you'll need a unique code sent to your phone or email to log in.
- **Monitor Your Accounts Regularly:** Check your bank statements and credit reports frequently for any suspicious or unauthorized transactions. Sign up for SMS alerts for all transactions.
- **Shred Sensitive Documents:** Securely shred any documents containing personal information, such as junk mail with credit card offers, bank statements, or loan applications.
- **Protect Your Devices:** Keep your computer, smartphone, and other devices updated with the latest software and security patches. Install genuine antivirus/anti-malware software and update it regularly.
- **Lock Your Devices:** Use a strong PIN, password, or biometric lock (fingerprint, facial recognition) to secure your devices.

Online and Digital Banking

- **Type URLs Manually:** Always type your bank's official website address directly into your browser. Never click on a link from an email or text message.
- **Look for Secure Websites:** Before entering any personal or financial information, ensure the website URL starts with "https://" and has a lock icon in the browser's address bar. The "s" stands for secure.
- **Be Careful with Public Wi-Fi:** Avoid conducting financial transactions on public, unsecured Wi-Fi networks. If you must, use a VPN (Virtual Private Network) to encrypt your data.
- **Clear Your Browsing Data:** After an online banking session, clear your browser's cache and cookies to prevent your information from being stored.
- **Log Out Properly:** Always sign out of your online banking account when you're done. Never leave an active session unattended.

Flipkart Finance Private Limited

Fraud Prevention

Don'ts for Preventing Banking Fraud

Sharing Information and Responding to Requests

- **Never Share Sensitive Information:** Do not share your bank account number, credit/debit card details, CVV, PIN, OTP, or passwords with anyone. Your bank will never ask for these.
- **Don't Respond to Suspicious Messages or Calls:** Do not click on links in unsolicited emails or text messages. Do not answer calls from unrecognized numbers, and never provide personal information to a caller, even if they claim to be from your bank.
- **Don't Download Unknown Apps:** Do not install applications or software from unverified sources. They may contain malware designed to steal your data.
- **Don't Give Remote Access:** Never grant remote access to your computer or mobile device to an unknown person, especially if they call claiming to be from tech support or your bank.

Social Media and Public Behavior

- **Don't Share Personal Information on Social Media:** Be careful about what you post online. Scammers can use details like your birthday, pet's name, or vacation plans to guess your passwords or target you for scams.
- **Don't Accept Unknown Requests:** Be cautious of friend requests or messages from strangers on social media, as they can be used for scams, including romance scams.

Transaction and Account Management

- **Do Not Make Payments to Unknown People:** Do not transfer money to unverified accounts or individuals. Be especially careful if someone you don't know asks for money.
- **Do Not Trust "Too Good to Be True" Offers:** Be skeptical of any offer that seems unusually lucrative, such as a lottery win or a high-return investment, especially if it requires you to pay a fee upfront.
- **Do Not Use Public Wi-Fi for Banking:** As mentioned in the "Do's," this is a critical security risk.
- **Do Not Pay Directly for Accidental Deposits:** If you receive money in your account from an unknown source, do not transfer it back directly to the sender. This can be a scam. Instead, contact your bank and let them handle the reversal.