Privacy Policy

What we collect

At Manappuram Home Finance Limited (MAHOFIN), we may collect the following information:

- Name and job title
- Including contact information email address
- Demographic information such as postcode, preferences and interests
- Other information relevant to customer surveys and/or offers

What we do with the information we gather

We require this information to understand your needs and provide you a better service's and for the following reasons:

- Assessing your profile while granting loan • Internal record keeping.
- demographic information such as postcode, preferences and interests.
- We may periodically send promotional emails about new products, special offers or other information of MAHOFIN which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your interests.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

How to use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added, and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website / any application in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Controlling your personal information

You may choose to restrict the collection or use of your personal information in the following ways:

- Whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes.
- If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to or emailing us.

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

If you believe that any information, we are holding on you is incorrect or incomplete, please write to us or email us as soon as possible. We will correct any information found to be incorrect.

Security Tips

Mobile/Electronic Device Security – Do's and Dont's

- Password protect the mobile phone and never give your mobile phone to anyone.
- Choose a strong password to keep your account and data safe.
- Do not share your One Time Password (OTP) to any one other than the transaction
- Change your mobile PIN regularly at least once in every 60 days.
- Report a lost or stolen phone immediately to your mobile service providers (For eg:

Airtel / Vodafone / Idea /BSNL etc.) and law enforcement authorities.

- Use anti-virus, anti-spyware and personal firewalls and keep them updating regularly.
- Use licensed software. Software purchased from untrustworthy sources could have virus or trojans that could corrupt your files and reveal your confidential data. • Don't store sensitive information such as credit card details, mobile banking password and user ID on your phone

Be cautious while open/download emails or attachments from known or unknown sources

- Be cautious while using Bluetooth/WiFi in public places as someone may access your confidential data/information
- Don't click on links embedded in emails/social networking sites claiming to be from the bank or representing the bank
- Be careful about the websites you are browsing, if it does not look authentic, do not download anything from it
- Update your mobile with latest security patches for your operating system, browser and email client.

Password Security tips

- When you receive your OTP, change it immediately. • Never use the following for your password: • Your kids' or loved ones' date of birth or anniversary • Consecutive numbers like 123456 or 987654
- Same numbers like 111111 or 444444 or 000000
- First or last digits of your card number / mobile number • Same password as of your mobile pin or password • Never share your password with anyone.
- Avoid using the same password for several different accounts. Once hackers have guessed one password, they'll often try to see if it works on other accounts.
- Memorize your password. Don't write down your password anywhere. • Change your password at regular intervals at least once in 60 days.
- If you suspect that someone knows your PIN/Password, change it immediately. • Don't send your password to anyone via email or text message.
- Don't say your password aloud in public where other people can hear you.
- Don't have your browser/mobile remember your account password.

Fraud Scenarios

Forged Phone Calls

Forged phone call is one such attempt where fraudsters possess as your relative / friend / Banker and ask your banking / credit card detail and ask for transfer the funds on immediate basis in their bank account/wallet.

How do fraudsters operate?

- Fraudster collects information about you from social networking sites like Facebook, Linkedin, twitter etc.
- Fraudster calls customer and poses as a relative or friend and talk to you about few scenarios which recently happened with you so that they can trick you in thinking that you actually know them.
- Once they get confidence that you are in trap, they ask you to transfer some money (usually small amount ranging between INR 500 to 5000) in their bank account or wallet account citing medical reasons.

Once customer transfer the amount fraudster further transfer that money to some other account so that transaction cannot be reversed.

How to protect yourself from fraud: • Never share personal details on social networking sites.

- Never transfer the funds without confirming the identity of the recipient as the money once transferred cannot be reversed.
- All your details like Name, Father name, date of birth, Mother name, bank / credit / debit card details, passwords are shall be kept confidential.

Phishing

Phishing is a type of fraud that involves stealing personal information such as Customer ID, OTP/Password, etc. through emails that appear to be from a legitimate source.

How do fraudsters operate?

- Fraudsters send fake emails to customers which appears legitimate, asking them to urgently verify or update their account information by clicking on a link in the email.
- Clicking on the link directs the customer to a fake website that looks like the official website – with a web form to fill in his/her personal information.
- Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to protect yourself from fraud:

- Always check the web address carefully.
- For logging in, always type the website address in your web browser address bar.
- Install the anti-virus, antispyware, firewall and security patches on your computer and mobile phones and keep updating them regularly.
- DO NOT click on any suspicious link in your email.
- DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard etc.
- DO NOT open unexpected email attachments or instant message download links
- DO NOT access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

How to identify fake Phishing website / Mails?

- Always check for the salutations in the mail, phishing mails are normally targeted to large audience, so they put generic salutation like below, genuine mail always comes with your name. o Dear Sir / Madam o Dear Customer
- Check the domain or email ID from where mail has come, generally fraudster try to build look alike email ID with some spelling changes.
- Such mails come with some kind of urgency and they threat you for some consequence if you ignore the mail.

When you click on URL it will redirect you to some website which will look alike the bank site but if you check the URL address then it would be different from bank site address.

- Most fake web addresses start with 'http://'. Legitimate site will always start with HTTPS, the 's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption.
- Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.
- Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window.

Vishing

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call

How do fraudsters operate?

- The fraudster poses as an employee from the bank or a Government / Financial institution and ask customers for their personal information.
- They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashing of reward points, sending a new card etc.

- These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from fraud:

- Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email.
- If in case of doubt, call to customer care of respective service provider for clarification.

Smishing

Smishing is a type of fraud that uses mobile phone text messages (SMS) to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

- Fraudsters send SMS intimating customer's of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials.
- Unaware, the customer's follow instructions to visit a website, call a phone number or download malicious content.
- Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

How to protect yourself from fraud: • Never share your personal information or financial information via SMS, call or email.

- Do not follow the instructions as mentioned in SMS sent from untrusted source, delete such SMS instantly.
- If you receive any urgent communication asking for personal information, call to respective service provider customer care, to check if it was a legitimate communication.

Identity Theft

Identity Theft occurs when someone wrongfully uses your personal information to obtain credit, loans and other services in your name.

How do fraudsters operate?

- They try to gather customer's details through Phishing, Vishing, Smishing or any other means.
- They call customers and try to collect details by posing as Bank Staff.
- They might visit customers posing as bank staff and collect personal information like Name, Father's Name, Address, Permanent Address, Date of Birth, Aadhaar number, PAN Number etc.

How to protect yourself from fraud: • Destroy any piece of paper holding details of your identity.

- Never share your personal information with a stranger or any third party, posing as bank representative.
- Update your bank records whenever you change your contact numbers, address or email ID.

SIM Swap

Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

How do fraudsters operate?

- Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.
- They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.
- The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.
- Fraudsters then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

How to protect yourself from fraud:

- If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam.
- Register for SMS and Email Alerts to stay informed about the activities in your account. • Regularly check your bank statements and transaction history for any irregularities.

Money Mule

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s).

How do fraudsters operate?

- Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.
- The fraudsters then transfer the illegal money into the money mule's account. • The money mule is then directed to transfer the money to another money mule's account – starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- When such frauds are reported, the money mule becomes the target of police investigations.

How to protect yourself from fraud:

- Do not respond to emails asking for your account details.
- For any overseas job offer, first confirm the identity and contact details of the employing company.
- Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.

Trojan

A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.

How do fraudsters operate?

- Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people
- Customers who open or download the attachment in these emails get their computers / mobiles infected.
- When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.
- These details will then be used to conduct fraudulent transactions on the customer's account.

How to protect yourself from fraud:

- Never open e-mails or download attachments from unknown senders. Simply delete such emails
- Installing antivirus helps. It scans every file you download and protects you from malicious files.
- Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.
- Install patches from software manufacturers as soon as they are distributed. A fully patched computer / mobile behind a firewall are the best defence against Trojan.
- Download and use the latest version of your browser.
- If your computer / mobile gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. If necessary, get your computer serviced.