Security & Privacy Policy

Your Privacy is very important to Fincare Small Finance Bank Limited (hereinafter referred to as "Fincare/Bank"). At Fincare, we value and recognize that one of the Fundamental Responsibilities is to protect personal information entrusted to the bank by its customers.

The Privacy Policy is in compliance with the Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules 2011 (the "IT Rules") contained in the Information Technology Act 2000.

Applicability:

This policy is applicable to all personal/business information of natural persons ("Individuals") collected or received directly from the Corporate or through Bank's online Portal, Electronic communications as processed or stored or dealt with or handled by Fincare

Policy Coverage:

This policy covers the "Sensitive personal/business data or information" of the individuals collected or received or processed or stored or dealt or handled by FINCARE in any form or mode.

Sensitive personal/business data or information covers passwords, financial information including banking related information, financials and credit information, ethnicity, caste, race or religion, health related details of the individuals, sexual orientation, medical records and history, biometric information or any other details provided by customers for providing banking services by Fincare ("Personal/business information") provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal/business data or information for the purposes of this policy.

Policy statements:

1. By providing the personal/business information, the individuals provide consent to FINCARE to use the personal/business information for the usage of the information for the product or services requested or applied or shown interest in and or to enable FINCARE the Individuals verification and or process applications, requests, transactions and or maintain records as per internal or legal or regulatory requirements and shall be used to provide the Individuals with the best possible services or products as also to protect interests of FINCARE.

2. The Information of its customers shall not be disclosed or shared with any external organisation or Third Parties unless the same is necessary to protect the interests of FINCARE or to enable FINCARE to provide you services or to enable the completion or compilation of a transaction, credit reporting, or the same is necessary or required pursuant to applicable norms or pursuant to the terms and conditions applicable to such Information as agreed to with FINCARE or pursuant to any requirement of law or regulations or any Government or court or other relevant authority's directions or orders.

3.The Information may be disclosed without obtaining Individuals prior written consent, for those information shared with government agencies mandated under the law to obtain information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences, or where disclosure is necessary for compliance of a legal obligation. Any Information may be required to be disclosed to any third party by FINCARE by an order under the law for the time being in force.

4. It may be necessary to disclose the Individuals information to one or more agents and contractors of FINCARE and their sub-contractors, but such agents, contractors, and sub-contractors will be required to agree to use the information obtained from FINCARE only for purposes hereinbelow.

5. Personal/business data or Information provided by you are retained (for later use) (i) as long as the purposes for which such data were collected continue Or (ii) for such period so as to satisfy legal, regulatory or accounting requirements or to protect FINCARE's interests.

6. Fincare shall have processes in place to ensure that the information residing with it is complete and accurate. The Individuals would ensure the accuracy of the information provided. If there are any changes or updation of the same, it shall be communicated to FINCARE.

7. The Individual authorises FINCARE to exchange, share, part with all information related to the details and transaction history of the Covered Persons to its Affiliates or banks or financial institutions or credit bureaus or agencies or participation in any telecommunication or electronic clearing network as may be required by law, customary practice, credit reporting, statistical analysis and credit scoring, verification or risk management or any of the aforesaid purposes and shall not hold FINCARE liable for use or disclosure of this information.

8. Fincare reserves the right to change or update this Privacy policy from time to time with reasonable notice to the customers on its website.

Effective Date: This Privacy Policy was updated as on 25-10-2017 and is effective as of that date.

About Phishing (Potential Security Threats):

'Phishing' is a common form of Internet piracy. It is deployed to steal users personal and confidential information like bank account numbers, net banking passwords, credit card numbers, personal identity details etc. Later the perpetrators may use the information for siphoning money from the victim's account or run up bills on victim's credit cards. In the worst case one could also become the victim of identity theft. A few customers of some other Indian banks have been affected by the attempt of phishing.

We would like you to be aware of methodologies in a 'Phishing' attack, do's and don'ts in sharing of personal information and the action to be taken in case you fall prey to a phishing attempt.

Methodologies:

- Phishing attacks use both social engineering and technical subterfuge to steal customers' personal identity data and financial account credentials.

- Customer receives a fraudulent e-mail seemingly from a legitimate Internet address.
- The email invites the customer to click on a hyperlink provided in the mail.
- Click on the hyperlink directs the customer to a fake web site that looks similar to the genuine site.
- Usually the email will either promise a reward on compliance or warn of an impending penalty on non-compliance.
- Customer is asked to update his personal information, such as passwords and credit card and bank account numbers etc.
- Customer provides personal details in good faith. Clicks on 'submit' button.
- He gets an error page.
- Customer falls prey to the phishing attempt.

Dont's:

1. Do not click on any link which has come through e-mail from an unexpected source. It may contain malicious code or could be an attempt to 'Phish'.
2. Do not provide any information on a page which might have come up as a pop-up window.
3. Never provide your password over the phone or in response to an unsolicited request over e-mail.
4. Always remember that information like password, PIN, TIN, etc are strictly confidential and are not known even to employees/service personnel of the Bank. You should therefore, never divulge such information even if asked for.

Do's:

1. Always logon to a site by typing the proper URL in the address bar.
2. Give your user id and password only at the authenticated login page.
3. Before providing your user id and password please ensure that the URL of the login page starts with the text 'https://' and is not 'http:// '. The 's' stands for 'secured' and indicates that the Web page uses encryption.
4. Please also look for the lock sign (🔒) at the right bottom of the browser and the Verisign certificate.
5. Provide your personal details over phone/Internet only if you have initiated a call or session and the counterpart has been duly authenticated by you.
6. Please remember that the bank would never ask you to verify your account information through an e-mail.

What to do if you have accidentally revealed password/PIN/TIN etc:

If you feel that you have been phished or you have provided your personal information at a place you should not have, please carry out the following immediately as a damage mitigation measure:

- o Change your password immediately.
- o Report to the bank by calling customer care numbers on our website.
- o Check your account statement and ensure that it is correct in every respect.
- o Report any erroneous entries to the bank.
- o Use the other compensatory controls provided by the bank like setting the limits for trusted third parties to zero, enabling high security, etc to minimize the risk.