DIGITAL PAYMENT

Contents

1 TERMS & CONDITIONS

These terms and conditions apply to the Customer who uses Digital Payment Service using the platform of service provider/s for repayment of Loan or any other charges to BELSTAR. Kindly read these terms and conditions carefully. By authorizing a payment to BELSTAR through the Digital Payment Service option("the service"), it would be treated as a deemed acceptance to these terms and conditions. BELSTAR reserves all the rights to amend these terms and conditions at any time without giving prior notice. It is the responsibility of the Customer to read the terms and conditions before using the Service

1.1 KEY TERMS:

The following is a summary of the key terms of this service:

1. Payment(s) through this Service may only be made with a Debit card (Master / Visa / RuPay / Maestro), Net-Banking, & UPI (Unified Payments Interface)
2. The Debit card, Net-Banking & UPI information provided by the customer at the time of using the service is processed by the payment gateway of the service provider only. It is the sole responsibility of the Customer to ensure that the information entered in the relevant field/s is correct. It is recommended that the customer should keep the transaction acknowledgement for record purpose, which might assist in resolution of any disputes that may arise out or usage of the service in future.
3. The Customer agrees, understands and confirms that his/ her personal data including, inter-alia, details relating to Debit card / Net – banking & UPI transmitted over the Internet Payment Gateway may be susceptible to misuse, hacking, theft and/ or fraud and that BELSTAR or the Digital Payment Service Provider(s) have no control over such matters.
4. The service is provided using a Payment Gateway of Service Provider through a secure website. However, neither the payment gateway of service provider nor BELSTAR gives any assurance, that the information so provided online by the Customer is secured or may be read or intercepted by a third party. BELSTAR does not accept or assume any liability in the event of such unauthorized interception, hacking or other unauthorized access to information provided by the Customer.
5. BELSTAR and/or the Digital Payment Service Provider shall not be liable for any inaccuracy, error or delay in, or omission of (a) any data, information or message, or (b) the transmission or delivery of any such data, information or message; or (c) any loss or damage arising from or occasioned by any such inaccuracy, error, delay or omission, non-performance or interruption in any such data, information or message. Under no circumstances shall BELSTAR and/or the Payment Service Provider, its employees, directors, and its third party agents involved in processing, delivering or managing the Services, be liable for any direct, indirect, incidental, special or consequential damages, or any damages whatsoever, including punitive or exemplary action arising out of or in any way connected with the provision of or any inadequacy or deficiency in the provision of the Services or resulting from unauthorized access or alteration of transmissions of data or arising from suspension or termination of the Service.
6. The Customer agrees that BELSTAR or any of its employees will not be held liable for any loss or damages arising from the use of Internet Payment Gateway of Service Provider, or reliance upon the information contained on the Website, or any failure to comply with these Terms and Conditions.

1.2 PRIVACY POLICY:

1. The information provided by the user related to payments using Debit card/ Net-Banking/ UPI is not accessed or stored by BELSTAR.
2. If payment is made by means of a Debit Card/ Net-Banking/UPI code that the Customer does not personally own, the permission of the owner of the above said Debit Card/ Net-Banking/UPI code must always be obtained by the customer to make payments. In using this facility the customer confirms that he/she has such permission.
3. No Warranty: The information and materials contained in this site including, graphics, links or other items are provided as on "As Is" and "As Available" basis by BELSTAR which is organized and tries to provide information accurately and expressly, disclaims liability for error or omission in this information and materials. No warranty of any kind, implied, express or statutory shall be given by BELSTAR and it shall not be limited to the warranty of fitness for a particular purpose and freedom from computer virus is given in conjunction with the information and materials.
4. Limitation of Liability: In no event, BELSTAR will be liable for any damage direct or indirect losses or expenses arising in connection with the Digital Payment Service Platform or use thereof or inability to use by any person or delay of operation or transaction, or non- functioning of the computer/ mobile/ electronic devices or virus/ similar attack etc.
5. The Customer authorizes BELSTAR to exchange, share, part with all information related to the details and transaction history of the Customers to its Affiliates / Subsidiaries / banks / financial institutions / credit bureaus / agencies/ Service Provider for 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 and shall not hold BELSTAR liable for use or disclosure of this information.

1.3 SECURITY:

BELSTAR shall not be liable for any failure by the Customer making payment to properly protect data from being seen on their screen by other persons or otherwise obtained by such other persons, during the Digital Payment processor or in respect of any omission to provide accurate information in the Course of the Digital Payment Process.

1.4 NON – BINDING

Please note that this privacy policy does not create any contractual or other legal rights in or on behalf of any party vis-à-vis Belstar nor is it intended to do so.

1.5 PROHIBITED ACTIONS

While using this Digital Payment Service Platform, User agrees not to, by any means (including hacking, cracking or defacing any portion of the Digital Payment Service Platform) indulge in illegal or unauthorized activities including the following:

- Restrict or inhibit any authorized user from using this Digital Payment Service Platform.
- Use the Digital Payment Service Platform for unlawful purposes.
- Harvest or collect information about Digital Payment Service Platform users without their express consent.

- "Frame" or "mirror" any part of the Digital Payment Service Platform without our prior authorization.
- Engage in spamming or flooding.
- Transmit any software or other materials that contain any virus, time bomb, or other harmful or disruptive component.
- Remove any copyright, trademark or other proprietary rights notices contained in the Digital Payment Service Platform.
- Use any device, application or process to retrieve, index, "data mine" or in any way reproduce or circumvent the navigational structure or presentation of the Digital Payment Service Platform.

1.6 TRANSACTION CHARGES

The transaction charges for using this Digital Payment Service will be borne by Belstar and No charge is payable by the user.

1.7 VARIATIONS TO THE TERMS AND CONDITIONS

BELSTAR reserves the right to vary these Terms and Conditions from time to time and the current version will be that published on this website. We reserve the right to decline the acceptance of an Digital Payment Service if the user's account is in default for any reason. BELSTAR may also make additions/deletions/alterations to the services offered, at its sole discretion. Belstar reserves the right to withdraw the service at any time at its discretion. Belstar retains the right to change the terms and conditions for Digital Payment Service, without any prior notice.

2 BEWARE OF FRAUD

In a time when digital is the most frequently used medium, especially for financial transactions, it has become even more imperative to safeguard ourselves against fraudulent behavior.

We urge the users therefore to take constant care of their key relationship co-ordinates with Belstar (e.g. Loan Account number, other personal details/ confidential information, etc.) and not share them with anyone. Further, we encourage the users to not entertain any communication (phone call, email, SMS) which prompts them to share their key personal details.

Users may receive communication asking them for sensitive information like Password, Customer ID, Debit Card details, OTP, etc. Any such Phone call/Email/SMS is an attempt to fraudulently transact from users account. Please be aware of such fraudulent Phone call, email or SMS.

2.1 Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords / Login Credentials, and credit/ debit card details (and, indirectly, money), often for malicious reasons (usually to carry out various types of financial fraud), by disguising as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using bait in an attempt to catch a victim. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to

the legitimate one. Communications purporting to be from social web sites , auction sites, banks, online payment processors or through phone call or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.
An attacker masquerades as a trusted entity, such as a bank, government, ISP (Internet Service Provider), web site, and tries to trick people into giving up their private information. These attacks often take the form of "urgent" emails asking people to take immediate action in order to prevent some impending disaster. Examples include topics such as the following:

- "Our bank/ company has a new security system. Update your information now or you won't be able to access your account."
- "We couldn't verify your information; click here to update your account."
- Sometimes the email claims that something awful will happen to the sender (or a third party), as in "The sum of Rs. / USD ********* is going to go to the Government / Trust unless you help me transfer it to your bank account."

People who click on the links in these emails/test may be taken to a phishing site – a web page that looks like a legitimate site they've visited before, but is actually controlled by an attacker/hacker. Because the page looks familiar, people visiting these phishing sites enter their username, password, or other confidential information on the site. What they've unknowingly done is given a third party all the information needed to hack their account, steal their money, or open up new lines of credit in their name. They just fell for a phishing attack.

The concept behind such an attack is simple: Someone masquerades as someone else in an effort to deceive people into sharing personal or other sensitive information with them. Phishers can masquerade as just about anyone, including banks, email and application / Service providers, online merchants, online payment services, and even governments. And while some of these attacks are crude and easy to spot, many of them are sophisticated and well-constructed. That fake email from "your bank/ company" can look very real; the bogus "login page" you're redirected to can seem completely legitimate. These emails have no connection with Belstar and Belstar does not use any such methods.

If you think you may have encountered a phishing site, please contact us at bml@belstar.in or call us at toll free: 1800-102-7049 with the relevant details.

Our company accepts no liability for the content of such emails, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

2.1.1 AVOID BECOMING A VICTIM OF PHISHING ATTACKS BY FOLLOWING THESE SIMPLE RULES:

The good news is that there are things customer/s can do to steer clear of phishing attacks and phishing sites:

- **Be careful about responding to emails that ask Customer/s for sensitive information.** Customer/s should be wary of clicking on links in emails or responding to emails/text messages that are asking for things like account numbers, usernames and passwords, or other personal/confidential information. We at Belstar do not ask for this information via email.
- **Go to the site yourself, rather than clicking on links in suspicious emails:** If you receive a communication asking for sensitive information but think it could be legitimate, open a new browser window and go to the organization's website as you normally would (for instance, by using a bookmark or by typing out the address of the organization's website). This will improve the chances that you're dealing with the organization's website rather than with a phisher's website, and if there's actually something you need to do, there will usually be a notification on the site. Also, if you're not sure about a request you've received, please contact us at bml@belstar.in or call us at toll free : 1800-102-7049
- **Be wary of the "fabulous offers" and "fantastic prizes" that Customer/s will sometimes come across on the web:** If something seems too good to be true, it probably is, and it could be a phisher trying to steal customer information. Whenever Customer/s come across an offer online that requires them to share personal or other sensitive information to take advantage of it, be sure to ask lots of questions and check the site asking for their information for signs of anything suspicious.
- **Use a browser that has a phishing filter:** The latest versions of most browsers include phishing filters that can help customer/s spot potential phishing attacks.
- **Do not reply** (without confirming the legitimacy of the source) to e-mails requesting for financial information, Customer information, Account information, Personal or any other confidential information etc., **such mails seems to come from legitimate source** but usually are meant to persuade user to send confidential data which is later used for malicious intents.
- **Do not use a link in an e-mail to get to a web page,** instead, type in the URL directly into your browser's address bar.
- **Be vigilant when downloading e-mail** attachment on your computer. If in doubt, do not download.

2.2 Vishing

Vishing works like phishing but does not always occur over the internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VOIP (Voice over IP), or landline or cellular telephone.

2.2.1 AVOID BECOMING A VICTIM OF VISHING ATTACKS BY FOLLOWING THESE SIMPLE RULES:

What does fraudster wants?

By impersonating as a trustworthy entity over call (Telephone / Mobile / IVR – Interactive Voice Response), the fraudster attempts to acquire sensitive information such as:

- Banking PIN
- CVV / OTP / ATM PIN / Internet banking password
- Credit / Debit card and personal financial details

Beware when you get a call from an unknown caller saying…?

- "Share bank account details so that the income tax refund can be transferred to it"
- "Card has been temporarily blocked and to avoid permanent blocking, do the following" do as directed or else card will be deactivated

How can you protect yourself?

- Never share confidential details like card number /Card expire date / CVV / OTP / Internet banking password / ATM PIN / Phone-banking pin with anyone
- Review your credit and bank statement regularly
- Always visit websites by typing URL in the address bar
- Ensure the website uses encryption technology
- Report suspected abuse to designated authorities

Belstar does not request for personal account information or any other related information by text message, email, or automated phone call.

Do not respond to any unsolicited texts, emails, pop-ups, or links that ask for personal information of any kind.

3 Reversal Policy

3.1 When the Customer has made payment but Credit is not update in Loan

This is a scenario, where customer has processed the payment using Debit Card/ Internet Banking or UPI for the EMI/ Charges raised to customer for the due demand; but the same has not been updated in the loan account of the customer. In this scenario, customer can raise the complaint to Toll free number- 1800-102-7049 Or email to bml@belstar.in or reach out to the Belstar Branch from where customer has got a loan.

In the complaint the customer needs to provide the sms/ Bank Statement which depicts that the payment has been made towards the above said EMI/Charges raised by Belstar.

Once, Belstar receives the complaint, same will be verified against the settlement report and based on the findings, customer would be informed of the payment updated/ not to be updated against the customer loan account. The reason for not updating will be shared to customer.

If the complaint is found to be correct, the customer account will be updated with the paid/ settlement amount thereby impacting or reducing customer loan balance.

3.2 When Credit is provided to incorrect account

This is the scenario where Customer-A has made the payment but the credit was made in system against the Customer-B; in which case as soon as Belstar finds the discrepancy, efforts will be made to rectify the same.

Customer-B in turn will also receive an SMS indicating that the payment was cancelled informing the updated Loan outstanding.

If any of the customer has any issues in this, same can be raised to Toll free number-1800-102-7049 Or email to bml@belstar.in or reach out to the Belstar Branch from where customer has got a loan.

4 General Terms:

1. The word Customer/ User/ Service Provider etc, wherever used in above text in singular will also mean plural, wherever appropriate.
2. Presently, IndusInd Bank Limited is our Service Provider for the aforesaid Digital Payment Service.
3. The word Belstar will mean Belstar Microfinance Limited.