बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

## Integrated Risk Management Department
## Head Office, Pune - 411005

11.01.2021

Dear Valued Customer,

Thank you for banking with Bank of Maharashtra!

Security of your account is of utmost importance to us. In our endeavor to continue educating our customers on security, we are hereby publishing the Customer Awareness - 21. Please find the same below. Hope you will find it useful and informative.

# Customer Awareness - 21

### Preventing potential cyber fraud due to card leakage

Security researchers have reported that Personal details such as email IDs, full names, phone numbers, and debit and credit card details of over a 100 million users of Juspay Payment Gateway Platform has been breached by cyber-criminals.

As per reports, it was found that the leaked information of the users was masked in some places to reveal only some part of card numbers. However, said data could still be used by the fraudster for phishing scams. Therefore, if you notice that your card has been compromised, call the Bank immediately (on 1800 233 4526) to Hotlist your card and visit your branch to issue a new card. You can also hotlist the card by using MahaMobile App or Internet Banking application of our Bank.

We also suggest you to follow the security practices as given under :

1. In the event that a hacker has made his way into your online account. Change your account password / PIN (Personal Identification Number) as soon as possible, so that no one other than you can perform transactions. Ensure that the password/PIN for each account/Card is different so that the hacker can't access all of them.
2. Approach local law enforcement agency for reporting of fraud in addition to Banks.
3. Ensure that you are regularly monitoring your account statement for suspicious transactions. Ensure that you have strong passwords/PINs for all accounts/Cards. Do not share your password/PINs with others. Change your card PIN periodically. Ensure your card is not enabled for International use, disable if it is not required.
4. Make yourself alert of any Phishing Scam that may take place using the leaked Data.