For private circulation only

GREATER BANK
The Greater Bombay Co-operative Bank Limited
(Scheduled Bank)

GREATER BANK TODAY

NEWS BULLETIN

ISO 9001 : 2008 Certified

Vol. 23 Issue No. 15 DECEMBER 2024

CHAIRMAN'S MESSAGE

MSME's: THE BACKBONE OF INDIA'S ECONOMIC FUTURE.

DEAR MEMBERS,

Micro, small, and medium enterprises (MSMEs) contribute significantly to India's total GDP and are one of the driving forces propelling the Indian economy towards global greatness. As per the Udyam portal, MSMEs employ over two crore people, firmly establishing themselves as the bedrock of the economy.

The government's objective is to raise this contribution from 30% to 50% in the coming years. Aided partly by supportive and reformatory government initiatives and technological innovations, the MSME sector has grown exponentially, accounting for ~46% of India's total exports.

To support and foster MSME, the Ministry of MSME has launched and implemented various schemes offering credit support, new enterprise development, formalisation, technological assistance, infrastructural development, skill development and training, and market assistance to MSMEs through initiatives like:

- Udyam Registration Portal: The government has come up with the facility of Udyam Registration Portal named to facilitate the permanent registration of MSME's through which they can generate Udyam Certificate which will enable MSME to access several government initiatives.
- Udyam Assist: The government has come up with the facility of Udaym Assist platform aimed to facilitate online registration Informal Micro Enterprise for generation of Udyam Registration Number and Udyam Assist Certificate, who may not have the necessary documents, motivation, ability or awareness to register on the Udyam Portal. We at Greater Bank have enabled our Branches to help existing and new customers for Udyam registration.
- Government E-Marketplace (GEM): MSMEs are being encouraged to market their products on the through GEM, owned and run by the government, wherefrom Ministries and PSUs (public sector undertakings) source their procurement.
- Launching of "CHAMPIONS" Portal: The government has launched "CHAMPIONS" Portal for redressal of MSMEs grievances, helping them with various government schemes/policies, providing guidance and advisory services in various areas like Finance, Technology, Infrastructure and Capacity Building etc.

THE DIGITAL TRANSFORMATION OF MSMES:

MSMEs are moving forward with renewed zeal and vitality and a decided focus towards innovation and digitisation of operational procedures. Adopting new tools and systems ensures a sharper edge to their global competitiveness. Moreover, schemes like the Digital MSME Scheme, which empowers all MSMEs registered with the Udyam registration portal to adopt Information Communication Technology (ICT) tools and applications in their production and operations, ensure that the transition from traditional processes to digital ones is as seamless as possible. Furthermore, the Ministry of MSMEs has been allocated INR 22,137.95 Cr under the interim Budget 2024-25 for implementing various schemes and technology upgrades.

CONCLUSION

MSMEs and a focus on their growth are critical for the long-term prosperity of India's economy. MSMEs play a crucial role in the GDP growth, industrial production, and job creation in the nation's economy, and the various initiatives and regulatory reforms fostering them are a step in the right direction to ensure that untapped talent, resources, and growth opportunities are brought to the foreground.

In the Current year Bank has aim to grow finance to MSME for which Bank has initiated following steps:

1. Introduced Loan Schemes for MSME.
2. Helping customer to register for Udyam Certificate through Udyam Assist Portal so that they can take benefit of various government schemes.
3. Create greater awareness among customer regarding MSME sector.

I request members who are already into MSME Sector or are willing to be part of the MSME sector to take the benefit of the bank's loan product and make us your partner in your growth journey.

With warm regards,

Dr. Narendrakumar A. Baldota

The classification of MSME is as follows :

1. a MICRO enterprise, where the investment in plant and machinery or equipment does not exceed one crore rupees and turnover does not exceed five crore rupees.
2. a SMALL enterprise, where the investment in plant and machinery or equipment does not exceed ten crore rupees and turnover does not exceed fifty crore rupees and
3. a MEDIUM enterprise, where the investment in plant and machinery or equipment does not exceed fifty crore rupees and turnover does not exceed two hundred and fifty crore rupees.

New Product on Flexi Overdraft (FOD) / Mortgage Loan (ML) for MSME
Annexure I

Sr. No.	Particulars	New Product	
		MSME – Mortgage Loan	MSME-Flexi Overdraft
1	Type	Mortgage Loan	Flexi Overdraft
2	Loan Amount	Min. ₹ 1.00 lakhs to ₹ 500.00 lakhs	
3	ROI	Interest @ 9.75% p.a. + additional risk based pricing	Interest @ 10.00% p.a. + additional risk based pricing
4	Purpose of Loan / End Use	Business requirements (expansion, start up - prior experience, diversification from existing business). Suitable documentary proofs to incur the expense to be submitted	
5	LTV	Self Occupied Residential Property – 75% Self Occupied Commercial / Industrial – 65% (LTV – 60% to be considered for property older than 15 years) Rented Property – 60%	
6	Eligibility	For Self Employed : • Residual income of applicant/s after deducting all the payouts including the proposed loan EMI to be 30% of monthly net income (Avg. of 3 months Net Salary/ GTI). A minimum of ₹10,000/- p.m. take home to be available. **OR** • LTV (mentioned above) of the Market Value of the property offered as Security as per the latest Valuation Report of bank's paneled valuer. Whichever is lower For ML - DSCR of 1.50 to 2	For Self Employed : • Residual income of applicant/s after deducting all the payouts including the proposed loan EMI to be 30% of monthly net income (Avg. of 3 months Net Salary/ GTI). A minimum of ₹10,000/- p.m. take home to be available. **OR** • LTV (mentioned above) of the Market Value of the property offered as Security as per the latest Valuation Report of bank's paneled valuer. Whichever is lower For FOD - ISCR of minimum 1.75 Eligibility to Flexi Overdraft (New Limits/ Enhancement): The facility sanctioned for business purpose should be justified based on the sales / turnover / MPBF of the applicant.

T&C Apply

For Purchase of Commercial Premises: The above product is extended for purchase of Commercial Premises by way of Term Loan. The following points are to be considered for granting Term Loan for purchase of Commercial premises under this scheme:

- Eligible borrowers - Partnership / Private Limited / Limited Liability Partnership / Limited with MSME registration.
- The purpose of purchasing the property is for business use only.
- Loan eligibility – 75% of the Agreement Value / Valuation, whichever is less.
- The property to be purchased should be fully constructed / ready to move with OC.
- Income Eligibility to be linked to existing cash accruals of the business.
- Deviation Approval : In case of FOIR deviation i.e. below 30% residual income, next level sanctioning authority or LCM.
- All other terms & condition will be as per the Scheme mentioned in this Annexure.

CYBER SECURITY AWARENESS

DO'S AND DON'TS FOR BANK CUSTOMERS

DO

GENERAL SECURITY

1. **Use strong, unique passwords and change them regularly.**
   Create passwords that combine letters, numbers, and special characters. Avoid using easily guessable information, such as birthdays or names. Regularly updating your passwords helps mitigate the risk of unauthorized access.
2. **Enable two-factor authentication (2FA) whenever possible.**
   2FA adds an extra layer of security by requiring not just a password but also a second form of verification, like a text message or authentication app.
3. **Keep your device's OS, browser, and antivirus software up-to-date.**
   Regular updates patch vulnerabilities that cybercriminals exploit. Ensure automatic updates are enabled to stay protected.
4. **Use reputable antivirus software.**
   A good antivirus program helps detect and block malware and other threats, providing peace of mind while you bank online.
5. **Back up important data regularly.**
   Regular backups ensure you can recover important information in case of data loss or ransomware attacks. Consider using both cloud storage and external drives.

ONLINE BANKING

1. **Use the bank's official mobile app or website.**
   Always download apps from official sources and access your bank's website directly to avoid phishing sites.
2. **Log in to online banking from a secure, private network.**
   Avoid using public Wi-Fi for banking transactions. Instead, use a secure home network or a virtual private network (VPN).
3. **Verify the website's URL (e.g., https://greaterbank.com).**
   Ensure the URL begins with "https" and check for a padlock icon in the address bar, indicating a secure connection.
4. **Check account activity regularly.**
   Routinely reviewing your account can help you spot unauthorized transactions early and address issues promptly.
5. **Set up account alerts and notifications.**
   Alerts for transactions and unusual account activity can help you monitor your finances in real-time, enabling quick action if needed.

EMAIL AND COMMUNICATION

1. **Verify sender details before responding to emails or messages.**
   Double-check email addresses and phone numbers. Phishers often use similar-looking addresses to trick users. (e.g., "paypal.com" instead of "paypa1.com" with a number one).
2. **Report suspicious emails or calls to the bank.**
   If you encounter anything unusual, inform your bank to help them investigate and prevent future scams.
3. **Register for the bank's SMS/Email alerts.**
   Alerts can keep you informed about account activities, changes, or potential security threats.
4. **Get Rich Quick Trading.**
   Social media ads promising high returns on stock investments.
5. **Reality.**
   High-return schemes are likely scams.

CARD SECURITY

1. **Sign your card immediately.**
   Signing your card helps protect against unauthorized use.
2. **Keep card details confidential.**
   Never share your card information, and be cautious when providing it over the phone or online.
3. **Report lost/stolen cards promptly.**
   Timely reporting can prevent unauthorized charges and secure your account.
4. **Monitor card transactions regularly.**
   Reviewing your statements/message (sms) can help you identify unauthorized charges quickly.

MOBILE SECURITY

1. **Use a secure lock screen and password/PIN.**
   A strong lock screen protects your personal data from unauthorized access.
2. **Install apps from trusted sources (e.g., App Store, Google Play).**
   Downloading apps only from official stores reduces the risk of malware.
3. **Keep your mobile OS and apps updated.**
   Updates often include security patches that protect against vulnerabilities.
4. **Use mobile security software.**
   Consider apps that offer additional security features, such as anti-theft protection and malware scanning.
5. **Do not click on any suspicious link.**

DON'T:

GENERAL SECURITY

1. **Don't use public computers or public Wi-Fi for banking.**
   These environments are often insecure and can expose your data to cybercriminals.
2. **Don't share sensitive info (OTP, password, card details).**
   No legitimate entity will ask you to share sensitive information via email or over the phone.
3. **Don't use weak passwords (e.g., name, birthdate).**
   Weak passwords are easy targets for attackers; always opt for stronger alternatives.
4. **Don't click on suspicious links or attachments.**
   These could lead to phishing sites or install malware on your device.
5. **Don't open e mails from unknown senders.**
   If you don't recognize the sender, it's best to delete the email without opening it.

CARD SECURITY

1. **Don't share card details via phone, email, or text.**
   This can expose you to fraud and unauthorized transactions.
2. **Don't sign blank transaction slips.**
   Always complete the slip before signing to prevent unauthorized charges.
3. **Don't keep card details written down.**
   Store this information securely and avoid carrying it with you.
4. **Don't ignore suspicious card transactions.**
   Report any unfamiliar charges to your bank immediately.

ONLINE BANKING

1. **Don't log in from unsecured networks (e.g., public Wi-Fi).**
   Always use a secure connection to protect your information.
2. **Don't use outdated browsers or operating systems.**
   Old software may lack critical security updates, making you vulnerable.
3. **Don't reuse passwords across multiple sites.**
   If one account is compromised, others could be at risk too.
4. **Don't leave online banking sessions open.**
   Log out of your account when finished, especially on shared or public devices.

ADDITIONAL TIPS

1. **Regularly review account statements.**
   Regular reviews can help catch errors or fraudulent activity early.
2. **Set up transaction limits.**
   Limiting transaction amounts can reduce potential losses in case of fraud.
3. **Use a secure wallet or card storage.**
   Digital wallets and secure physical storage can help protect your cards.
4. **Stay informed about the latest security threats.**
   Knowledge of current threats helps you recognize and avoid potential scams.

PHISHING AND SCAMS

1. **Don't respond to urgent or suspicious requests.**
   Legitimate organizations will not pressure you for immediate action.
2. **Don't provide sensitive info via phone, email, or text.**
   Always verify the identity of the requester before sharing any information.
3. **Don't click on links from unknown sources.**
   These could lead to malicious websites that compromise your security.
4. **Don't download attachments from unknown senders.**
   They may contain viruses or malware.

REPORT INCIDENTS

If you suspect any unauthorized transactions or security breaches:

1. **Visit the bank's nearest branch.**
   In-person communication can expedite the resolution process.
2. **Report to local authorities (if necessary).**
   This can help in cases of identity theft or larger-scale fraud.
3. **National cyber helpline number 1930.**

By following these Do's and Don'ts, bank customers can significantly reduce the risk of cyber threats and protect their financial information.

GREATER BANK

The Greater Bombay Co-operative Bank Limited
(Scheduled Bank)

UPI Payments

Faster and Secured Way of
Fund Transfer and Collection

amazon pay | Paytm | BHIM
G Pay | PhonePe | Pay

ONE STOP SHOP FOR ALL YOUR BANKING NEEDS

HOME LOAN	MORTGAGE LOAN	GOLD LOAN	CAR LOAN
OVERDRAFT	CURRENT A/C	SAVING A/C	FIXED DEPOSIT
DEMAT A/C	LOCKER FACILITY	INSURANCE	MUTUAL FUND

*Terms and conditions applied

For more details contact our nearest branch, visit our website www.greaterbank.com or email us to info@greaterbank.com