DALAL & BROACHA
STOCK BROKING PVT. LTD.

Dear Client,

Greetings of the day!

We refer to your investment account with us.

As an organization it is our constant endeavour to adopt best industry practices and ensure your account's safety and security to give you best investment experience. This email is intended to raise awareness and protect your interests.

- **Never give cash or transfer funds to Employee's / Authorized Person's personal account**

We do not accept cash or any money in any employees'/partners' personal account. Please do not make any payment in cash/employee/partners account. Please ensure the payment is made online or as account payee in the designated D&B (Dalal & Broacha) account.

- **Do not share your password / login details to anybody**

Please don't share your login credentials and OTP details with anyone. Also note that D&B employees / Authorized Person will not ask you to share your login details.

We do not accept cash or any money in any employees'/partners' personal account. Please do not make any payment in cash/employee/partners account. Please ensure the payment is made online or as account payee in the designated D&B (Dalal & Broacha) account.

- **SMS Stocks & Watch lists**

The list of securities in which unsolicited messages are being circulated ("SMS Stocks") are published from time to time on Exchange website thereby cautioning the market participants against SMS tips and to do thorough analysis about the company before investing. In the recent meeting of SEBI with Stock Exchanges and select trading members in this regard, it has been decided that;

- ✓ Sales proceeds shall be withheld for clients selling SMS Stocks and same will be transferred to the designated bank account earmarked for this purpose.
- ✓ There should not be any transactions in these scrips; likewise no exposure will be available for these scrips.
- ✓ The aforementioned shall also be made applicable to all SMS Stocks which may be published by the Stock Exchanges on its website from time to time.

Kindly refer to the Current Watch list / Historical Watch list / For information link for the list of Scrips from NSE and BSE

- **Beware of Malicious spam mail**

With the new normal work culture after outbreak of novel coronavirus (COVID-19) across the world - Cyber threats are looming at large and are constantly evolving in order to take advantage of online behaviour and trends. It is observed that - cybercriminals have been capitalizing on this by attacking computer networks, networks systems of individuals, businesses and even global organizations.

Additionally - malware, spyware and Trojans like Eventbot, Cerberus, Adwind JavaRAT, JsOutProx RAT are embedded in websites or are sent as spam emails to trick users to download malware to their computers or mobile devices. To update you, the malware abuses Android's in-built accessibility features to steal user data from financial applications, read user SMS messages and intercepts SMS messages allowing itself to bypass two-factor authentication. They could also use spear-phishing emails posing as either RBI or a large banking organization intending to influence the user to place their trust and click the links in the mail. With such an increase being noted, its' important for us to focus on cybersecurity, whether it's for yourself or your workplace.

We recommend the following Do's as guidelines to keep away from malicious e-mails / SMS

Do's

- Always check if the sender's email address looks different from their display name. example: where your service provider is Airtel but address looks like www.irtel.com etc.
- Check if the mail / SMS has spelling mistake or has grammatical errors or is unprofessionally drafted - this is a clear signal that it's a spam mail.
- Check if the mail is sent from unknown source/person or e-mail has unknown URLs.
- When downloading an app - Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
- Install apps downloaded from reputed application market.
- Avoid using unsecured, unknown Wi-Fi networks. There may be rogue Wi-Fi access points at public places used for distributing malicious applications.
- Transact on https websites only.
- Install and update your virus detector software always.

Dont's

- In settings, do not enable installation of apps from "untrusted sources".
- Never share your login id and password with any person.
- Do not click on the links of unknown users.
- Never reply to any e-mail/ SMS which asks you to confirm your personal details.

We at D&B recommend you to stay alert and refer to the **Security Best Practices issued by *Cyber Swachhta Kendra*** of Government of India by clicking here.

In case of any clarifications, please get in touch with your **Authorized Person / Relationship Manager/ Dealer** or write to us at info@dalal-broacha.com

Stay Alert - Stay Safe!

Warm Regards,

Team D&B