MasterCard Worldwide Security Guidelines: Phishing Scams

As email phishing attacks are growing in number (the term "phishing' refers to a scam and is the attempt to fraudulently acquire sensitive cardholder data such as logins and passwords), please keep in mind some tips that MasterCard Worldwide offers to protect against phishing.

To safeguard yourself against phishing:

- **do not disclose your sensitive personal information. A legitimate message from MasterCard and Baltic International Bank will be very specific and will never ask for your sensitive cardholder data such as your card number, PIN, 3D Secure Code, and CVV**;
- never click on links contained in the message. Rather, you should visit Bank's website or use our Internet Banking service, or call Bank's officer;
- refrain from opening and downloading suspicious email attachments;
- change the passwords periodically;
- if you are asked to provide you sensitive personal information used to identify you as a cardholder, please immediately report the fact to Bank;
- remember that phishing messages are often poorly written, with spelling and grammatical errors, and the messages instruct you to supply your account information (sensitive cardholder data). This is a clear indication that this is nothing more than a phishing scam. Links that are longer than normal, contain the symbol @ as a trap for the unwary or are misspelled could be signs of phishing. Phishing emails are designed to intentionally deceive you, and internet scammers know how to disguise their traps;
- only download files or open attachments in emails from known and trustful senders;
- if you are a victim of a phishing attack and believe your card may have been compromised, please contact Bank without further delay.

Phishing is a type of internet fraud. The term "phishing' refers to a scam and is the attempt to fraudulently acquire sensitive cardholder data such as logins and passwords. This is how it works: the phishers / fraudsters send bulk emails purporting to originate from well-known and trustful brands or from financial institutions (banks). Scammers also use social networks to steal identities. Email scams often urge you to click a link on the email to access a particular website. Once you are inside the fraudulent website, fraudsters may induce you to enter your username (also called login or loginID) and password to login to a certain website. Scammers use psychological tricks and triggers to impersonate the cardholder, steal sensitive cardholder data and get access to bank accounts.