MBOS and multiple safeguards taken

To ensure the security of MBOS, Metrobank provides multiple safeguards to protect, detect, respond, and recover against cyber-attacks, such as perimeter and network security, access controls, endpoint or device security, and application and data security.

Standard practices like regular risk and vulnerability assessment and third-party penetration testing are also performed on top of strong password requirements and multifactor authentication. Moreover, the following solutions prevent hackers from exploiting Metrobank facilities:

- **End to End data transmission is encrypted using 256-bit Secure Sockets Layer (SSL) encryption.** This certificate is among the most secure encryption methods for data transfer over a network or internet connection. It is the industry standard in encryption algorithm, protocol, and technology, including AES and SSL.

  This type of encryption is required for the most sensitive and important data, such as financial, military, or government data, because it is impossible to be decoded, even by the fastest computers. A hacker may attempt various combinations to break a 256-bit encrypted message, and still fail.

- **Malicious online activities are protected using Web Application Firewall (WAF).** While proxies generally protect clients, WAFs protect servers. It applies a set of rules for filtering, monitoring, and blocking Hypertext Transfer Protocol (HTTP) conversations. Generally, these rules cover common attacks such as cross-site scripting (XSS) and Structured Query Language (SQL) injection.

- **Servers are protected with Anti-Malware and Host-based Intrusion Prevention System (HIPS).** Anti-malware or Anti-virus and HIPS are systems or programs employed to protect critical computer systems that contain crucial data against viruses and other Internet malware. Starting from the network layer all the way up to the application layer, HIPS protects both the bank's and your information from known and unknown malicious attacks.

- **Security and system logs are collected, monitored and correlated using Log Management and Correlation System (LMCS) or Security Information and Events Management (SIEM) by 24x7 highly skilled Security Operations Center (SOC) personnel.** LMCS is a system used in collecting and organizing various system logs in the IT infrastructure of Metrobank. It is used in malware infection notification, denial-of-service alert, network intrusion alert, data leakage alert, and identity theft alert. Events and alerts are monitored by security threat analyst and incident responders to ensure timely and appropriate response.