TBC Bank JSC proposes the following amendments/additions to the Key Terms and Conditions of the E-Commerce Agreement (hereinafter the "Key Terms") and the Standard Terms and Conditions of the E-Commerce Agreement (hereinafter the "Standard Terms") in line with Paragraph 1.4 of the Key Terms of the E-Commerce Terminal Service Agreement published on the Bank's website https://www.tbcbank.ge/web/en/web/guest/card-payments:

1. **Paragraph 1.1 of the Key Terms be revised to read as follows:**

1.1 The Merchant (an entrepreneur/ individual taxpayer and/or a legal entity/ organizational entity) shall ensure that Visa and MasterCard international cards and TBC E-commerce and/or TPAY QR and/or GEOPAY are used as payment tools for accepting payments for goods/services;

2. **Paragraph 1.4 of the Key Terms be revised to read as follows:**

1.4 The Bank has the right to make amendments/additions to the provisions envisaged in this Agreement and/or set forth in any annex related to e-commerce services and/or any application related to e-commerce services and/or published on the Bank's website https://www.tbcbank.ge/web/en/web/guest/card-payments (hereinafter referred to as the "Bank Website") either by displaying relevant information on the Bank's website or sending a relevant notification to the Merchant 1 (one) month before the amendments/additions become effective. The Merchant may refuse to take the service envisaged in this Agreement by notifying the Bank thereof in writing within 1 (one) month of the date on which the information about the amendments/additions is displayed on the Bank's website or a relevant notification is sent to the Merchant. If the Merchant exercises its rights set out in this Paragraph, it shall settle all fees and other charges related to the service within 5 (five) calendar days of notifying the Bank in writing of its intention to cancel the service envisaged in this Agreement. The Agreement shall be valid until full settlement of all obligations assumed by the Merchant hereunder. If the Merchant does not exercise his/her/its right to terminate the Agreement, the amendments/additions proposed by the Bank shall be deemed accepted by the Merchant and the provisions/tariffs/charges shall be amended as proposed. The Bank can effect amendments/additions that do not deteriorate the Merchant's position as soon as they are published on the website/communicated to the Merchant in a notification.

3. **Sub-Paragraph 1.4.1 of the Key Terms be cancelled.**

4. **Paragraph 1.12 be added to the Key Terms to read as follows:**

1.12 This Agreement is an integral part of the Agreement on Banking Transactions made by and between the Bank and the Merchant / validated by the Merchant, which means that this Agreement is fully subject to the effect of the Agreement on Banking Transactions.

5. **Paragraph 1.1 of the Standard Terms be revised to read as follows:**

1.1 The definitions of terms and rules provided in the Agreement are compliant with the rules of international payment systems (payment network processors) VISA International and Mastercard Worldwide:

6. **The definition of the term "Authorization" set forth in Paragraph 1.1 of the Standard Terms be revised to read as follows:**

"**Authorization**" – for the purpose of this Agreement: a procedure whereby the availability of the necessary amount is checked in the card account and the amount is subject to a hold; a procedure for approving or rejecting a transaction request;

7. **The definition of the term "Chargeback" set forth in Paragraph 1.1 of the Standard Terms be revised to read as follows:**

"**Chargeback**" – a procedure whereby a card issuer or holder files a claim against a transaction and requests full or partial reversal from the acquiring bank (the bank in charge of processing the payment), in line with the rules of VISA International and Mastercard Worldwide and the Georgian legislation;

8. The definition of the term "International Payment System/Network" set forth in Paragraph 1.1 of the Standard Terms be revised to read as follows:

"**International Payment System/Network**" – international payment systems/networks VISA and Mastercard;

9. The definition of the term "Issuer" set forth in Paragraph 1.1 of the Standard Terms be revised to read as follows:

"**Issuer**" – an organization that issues and delivers to clients bank cards based on relevant agreements;

10. The definition of the term "Electronic Drafts" set forth in Paragraph 1.1 of the Standard Terms be revised to read as follows:

"**Electronic Drafts**" – an electronic set of transaction data generated by the Payment System/Network in the online store's system upon card payments. Electronic Drafts are the basis for settlement between the Bank and the Merchant.

11.Sub-Paragraph 2.1.1 of Article 2 of the Standard Terms be revised to read as follows:

2.1.1 Transfer transaction proceeds in the national currency to the Merchant's account provided by the Merchant to the Bank based on Electronic Drafts and to the deadlines specified in the Application/on the Bank's website;

12. Sub-Paragraph 2.1.2 of Article 2 of the Standard Terms be revised to read as follows:

2.1.2 Carry out the transfer mentioned in 2.1.1 based on the batch data after the transaction is processed in the card payment network;

13. Sub-Paragraph 2.1.4 of Article 2 of the Standard Terms be revised to read as follows:

2.1.4 Notify the Merchant regarding a fraudulent transaction no later than the following business day after it is informed about a fraud application and/or a chargeback filed with the card issuer.

14. Sub-Paragraph 2.1.5 of Article 2 of the Standard Terms be revised to read as follows:

2.1.5 Ensure that the transaction amount is transferred (settled) to the Merchant's account in compliance with the terms and conditions stipulated in the Agreement no later than the following business day.

15. Point 4 of Sub-Paragraph 2.2.1 of Article 2 of the Standard Terms be revised to read as follows:

4) Penalties imposed by the International Payment System/Network on the Bank due to an incident on the Merchant's part and/or by reason of the Merchant;

16. Sub-Paragraph 2.2.3 of Article 2 of the Standard Terms be revised to read as follows:

2.2.3 Provide the International Payment System/Network with any information about the Merchant known (available) to the Bank, if requested;

17.Sub-Paragraph 3.1.2 of Article 3 of the Standard Terms be revised to read as follows:

3.1.2 After the Bank ensures that the Merchant is registered as a payment system participant, display the information about card payment/settlement rules on the online store's website;

18. Sub-Paragraph 3.1.4 of Article 3 of the Standard Terms be revised to read as follows:

3.1.4 Pay the Bank the following amounts within 3 (three) business days of the Bank's notice:

- Reversals;
- Transactions disputed by the card issuer (chargebacks);
- Penalties/payments imposed by the International Payment System on the Bank due to an incident on the Merchant's part and/or by reason of the Merchant;
- Any type of loss/damage caused to the Bank due to incorrect/inaccurate information about the Bank spread by the Merchant.

19. Sub-Paragraph 3.1.6 of Article 3 of the Standard Terms be revised to read as follows:

3.1.6 Observe the International Payment Systems' requirements for the websites of e-commerce stores, which are provided in Annex #1.

20. Sub-Paragraph 3.1.7 of Article 3 of the Standard Terms be revised to read as follows:

3.1.7 Fulfil the requirements set forth in Sub-Paragraph 3.1.4 of the Agreement with respect to each authorized transaction within 180 (one hundred and eighty) days after the Bank transmits it to the International Payments Systems. Thus, the Bank reserves the right to deduct by direct debit the amounts indicated in Sub-Paragraph 3.1.4 hereof from the Merchant's Insurance Reserve and/or other accounts within 180 (one hundred and eighty) calendar days after an authorized transaction is transmitted by the Bank to the International Payments Systems;

21. Sub-Paragraph 3.2.3 of Article 3 of the Standard Terms be revised to read as follows:

3.2.3 Payment tools/gateway(s) mentioned herein are only used to accept payments for goods/services sold;

22. Sub-Paragraph 3.2.7 of Article 3 of the Standard Terms be revised to read as follows:

3.2.7 The Merchant implements anti-money laundering restrictions and measures and will adhere to the Law of Georgia on the Facilitation of Prevention of Illicit Income Legalisation as well as anti-money laundering regulations of the International Payment Systems (VISA/Mastercard);

23. 3.4 Paragraph (with Sub-Paragraphs 3.4.1-3.4.1.4) be added to Article 3 of the Standard Terms to read as follows:

3.4. The Merchant warrants and represents that:

3.4.1 Anytime before the execution of this Agreement or during the validity period hereof, the Client, its shareholders, management or the members of its executive/supervisory body, as well as the Client's beneficial owner(s) and/or the Parties affiliated therewith (including, for the purposes of this paragraph, any person that, according to the Bank's assessment and, inter alia, with regard to the purpose of the sanction(s), may have an influence on the person in question, or his/her/its decision(s) by way of close business, personal or other connections, and/or directly or indirectly hold and/or control that person:

3.4.1.1 are/will not be included in the list of the sanctioned persons (hereinafter the List of the Sanctioned Persons) by the United Nations (UN) and/or the European Union and/or the United Kingdom and/or the USA and/or Georgia and/or any other state and/or international organization (hereinafter jointly and individually referred to as the Authorized Person(s)), and/or is not/will not be subjected to a sanction (for the purposes of this paragraph, a sanction inter alia includes restriction, policy, prohibition, or other requirements set by the Authorized Persons).

3.4.1.2 Are not/will not be residents of a state subjected to the Authorized Person(s) comprehensive trade sanctions/restrictions.

3.4.1.3 Has not / will not enter into any deal (inter alia, will not facilitate execution of a deal), whether directly or indirectly, including through third party mediation, with any person and/or association that is/will be included in the List of Sanctioned Persons and/or is subjected to a sanction or is a resident of a state and/or operates on the territory subjected to comprehensive trade sanctions/restrictions.

3.4.1.4 Has not entered / will not enter into any deal (and/or facilitate execution of a deal), whether directly or indirectly, including through third party mediation, with regard to the party/property/asset/goods/services subjected to comprehensive and/or targeted and/or sectoral sanctions/restrictions.

3.4.1.5 If the statement/representation made pursuant to Paragraph 3.4 is found untrue and the Client's activity qualifies as a breach/evasion of sanction and/or according to the Bank's assessment, the aforementioned fact exposes the Client, its shareholders, member(s) of its management or executive/supervisory board and/or its beneficial owner(s) and/or person(s) affiliated therewith to a sanction risk or has resulted in sanctioning any of the aforementioned persons, along with actions stipulated herein, the Bank will be authorized to act pursuant to the sanctions imposed by the Authorized Person(s) indicated in Paragraph 3.4.1.1 hereof and take any and all measures set and/or required by the Authorized Person(s) and/or Entities/Bodies, inter alia, prevent the Client from using/disposing of and managing any funds/assets.

24. Paragraph 6.3 of Article 6 of the Standard Terms be revised to read as follows:

6.3. The Bank may terminate the Agreement at any time by giving the Merchant 1 (one) month's written notice. The Agreement shall be deemed terminated after all financial, organizational and technical matters are settled;

25. Paragraph 6.4 of Article 6 of the Standard Terms be revised to read as follows:

6.4. The Bank may revise terms and features of the services(s) described herein and/or the respective charges (if the Bank's tariffs change) and propose the Client or cancel any or several services envisaged by the Agreement or annexes hereto;

26.Paragraph 7.1 of Article 7 of the Standard Terms be revised to read as follows:

7.1. Unless otherwise envisaged by the effective law of Georgia, each Party undertakes not to disclose to a third party/ies without the other Party's written consent any information that directly or indirectly relates to the Agreement and is confidential. This obligation shall also apply after the termination of contractual relations.

27.**Paragraph 1 of Annex #1 of the Standard Terms be revised to read as follows:**
Rules/conditions set out in the Annex are binding on companies that use e-commerce or TBC E-commerce gateway to accept payments:

28. Annex #4 of the Standard Terms be revised to read as follows:

Annex #4

Privacy Policy

1.1. The Company represents and warrants that it will:
1.1. Process the data transferred to it in compliance with this Agreement and the Law of Georgia solely for the purpose indicated herein and defined by the Law of Georgia;
1.2. Take relevant technical and administrative measures with respect to the risks related to the nature of the data and the data subject in order to prevent unauthorized processing of personal data (including unauthorized dissemination, access, modification and destruction);
1.3 Liaise with the Bank for protecting the privacy of the data subject;
1.4 Observe and inspect/study any activity that violates requirements envisaged by the legislation, including international regulations, and will forthwith report to the Bank thereon;
1.5 Liaise with the Bank on addressing the data access issue on the data subject's request;
1.6 Adhere to legislative, including, international, regulations on privacy and ensure that the data subject's rights are protected;
1.7 Provide the Bank with all information that is necessary to meet regulatory requirements on privacy;
1.8 Allow the Bank or the auditor authorized by the Bank to carry out audit and/or inspection in order to establish if data processing is done appropriately;
1.9 If a data subject requests that his/her data processing be stopped, or wishes to exercises any of his/her other rights under the law (requests that his/her data be corrected, completed, updated, blocked, deleted, destroyed, etc.) or requests information regarding his/her data processing, including the following:
1.9.1 which of his/her data are being processed;
1.9.2 For which purpose;
19.3 What are the legal grounds of data processing;
1.9.4 How were the data collected;
1.9.5 To whom were his/her data transferred, on what grounds and for what purpose;
Forthwith, but no later than the next business day, notify the Bank thereof electronically at the email address privacycommitee@tbcbank.com.ge, wait for the Bank's instructions and deliver the requested information to the data subject, in a form requested by the latter, on the same day as the Bank issues the instruction. If the Bank does not respond to the Company's notification, the Company shall nevertheless give the requested information to the data subject. If this rule is breached, the Company shall bear the full responsibility.
1.10 Store the records of its data processing activities.
1.11 Limit access to personal data to a narrow circle of users/administrators and only grant access rights to those who have been duly instructed on privacy issues in advance, have an immediate need to access the data and are aware of non-disclosure/security requirements and ensure data secrecy protection, including in case of employment termination;

1.12 In case of accidental or unauthorized access to personal data, or destruction, loss, modification or disclosure thereof, inform the Bank immediately or not later than 2 (two) business days therefrom regarding the nature of the incident, indicating the data destroyed/lost/modified/disclosed. Furthermore, if possible, report to the Bank the category and exact amount of the data, as well as the way the breach occurred. The report must additionally contain contact information of the data protection officer and the channel through which additional information can be obtained;

1.13 Support the Bank in establishing the consequences of data breach;

1.14 Take immediate measures to ensure timely response to an incident and elimination of the causes, and inform the Bank about these measures;

1.15 Not transfer to a third party personal data received from the Bank under the Agreement without the Bank's prior approval. If such an approval is provided, requirements envisaged hereunder will apply to any third party receiving the data, without any limitations;

1.16 Not process personal data against the Bank's instructions, including in case of personal data transfer to a third party, a foreign state or an international organization; forthwith notify the Bank if the Bank's instruction is not compliant with legislative regulations or privacy&data protection requirements of any state;

1.17 In case of a dispute between the Parties, transfer to the Bank the data available to it;

1.18 Upon the Bank's approval, take special measures, considering the nature of the data and the risks associated with their transfer, especially if the data include information revealing a person's racial and ethnic origin, political opinions, religious or ideological/philosophical convictions, union membership, or unique identifier or identity marker. The obligation hereunder likewise applies to data concerning a person's heath, sex life, sex orientation or criminal record.

1.19 Not transfer personal data outside Georgia. If the Company's activities require cross-border data transfer, forthwith inform the Bank thereon via email at the address privacycommitee@tbcbank.com.ge and wait for the Bank's instructions. Anyway, data transfer to a third party is only allowed provided the data are transferred to a country that is on the Whitelist under the Georgian legislation and GDPR regulations.

1.20 On its own, without the Bank's approval, will not transfer data and/or consent to data transfer by a third party to a non-EU member state or outside EEA (European Economic Area). If the Bank gives its approval, it will be guided by EU general data protection regulations and will take special measures to protect personal data;

1.21 Assign personal data processing to subcontractors only on special occasions and upon the Bank's written approval. These subcontractors shall have in place relevant security solutions/protocols and be subject to the requirements envisaged hereunder, without any limitations. Assignment of personal data processing to subcontractors does not relieve the Company of its obligations or limit its responsibilities in case of damages resulting from the breach of the obligations;

1.22 If the Company hires a subcontractor in personal data processing, inform the Bank regarding the identity of the subcontractors and make changes related thereto only upon the Bank's written approval. The Bank is authorized not to approve the subcontractor proposed by the Company. Unless the disagreement is resolved through negotiations, the Bank is authorized to terminate the Agreement with the Party prematurely, without incurring any compensation liabilities;

1.23 If the Company winds up and/or the Bank terminates the agreement, return to the Bank and destroy/delete permanently the personal data transferred to it as well as copies thereof within a reasonable period of time. The Bank is authorized to require confirmation of deletion from the Party. This provision does not apply to information which the Party is obliged to maintain under the effective Law.

1.24 Obligations related to personal data processing remain in force following the completion of the contractual relationship up to the date to which the Contractual Party maintains access to personal data transferred to it. This provision shall not be construed as the Company's right to maintain access to personal data transferred to it under the Agreement after the completion of contractual relationship. The Company shall return and destroy/delete permanently personal data transferred to it by the Bank and copies thereof within a reasonable period after the completion of contractual relations but not later than 30 days;

1.25 If the local law prohibits deletion or return of data, the Company will remain the data possessor in line with this Policy and solely within the scope required by the local legislation;

2. In case of reasonable doubts, the Bank is authorized to check the performance of tools and systems used for processing personal data transferred to the Company, as well as their compliance with technical and administrative specifics under safety requirements set forth herein;

3. Depending on the gravity of the breach of the aforementioned guarantees, for the purpose of the inspection, the Bank has the right to demand relevant information and documents from the Company;

4. The Bank shall not be responsible for any damage and cost resulting from deliberate or negligent breach of any of

the obligations under this Policy;

5. The Company shall fully adhere to the following requirements of Information System Infrastructure as to the environment in which the personal data supplied by the Bank are hosted/ stored temporarily or continuously:

5.1 Personal data are to be stored and processed in a secure isolation domain separated by the main infrustructure by independent Firewall. The Firewall access must be controlled by duly authorized persons. The data stored/hosted in the secure isolation domain must be accessed via jump servers.

5.2 The integrity/accessibility of the isolation domain must be controlled and monitored;

5.3 Updates on servers in the isolated domain must be monitored.

5.4 Where possible, personal data must be encrypted by using cryptographically strong algorythms;

5.5 The isolation domain must be accessed by using protected methods, encypted communication and secure protocol.

5.6 A password policy must be in place for the isolation domain to define password complexity and change requirements and history settings.

5.7 Admin passwards to the isolation domain zone servers must be broken down at least into two parts and kept with different users by means of a secure method.

5.8 The Privileged Access Management System (PAM) must be in place to manage Admin passwords to the isolation domain.

5.9 Use access to the isolation domain must be subject to Two Step Authentication.

5.10 The isolation domain must not be accessible via the Internet. A login system must be installed on isolation zone servers. The logs must be saved and stored in a cetralized location and used as necessary for investigating an incident or an error.

5.11 Remote storage/ Cloud Service must not be used for storing, processing and transferring personal data.

5.12 When used for testing or development, the data must be distorted to prevent direct or indirect identification of the data subject.

5.13 The data must be shredded or incinerated after the expiration of the retention period or upon special request. The Bank's dedicated representative must be present at the processes of data destruction.

29. Annex 7 be added to the standard Terms and Conditions to read as follows:

Annex #7

The Rules/Terms hereunder are binding on the Merchants that operate online ecommerce platforms aimed at integrating vendors/service providers and customers into a single online site (hereinafter the "Marketplace") for the purpose of selling goods / providing services.

The Merchant shall:

1. Develop policies and procedures for (i) identifying vendors / service providers (as well as their beneficiary/ies) and customers / collecting information for further analysis / data tracking; (ii) verifying the truthfulness and accuracy of information obtained / collected as per (i). These policies and procedures shall be in line with the Law on Facilitating the Prevention of Money Laundering and Terrorism Financing / the applicable US, EU, UK and Georgian laws on the administration of international sanctions and monitoring of sanctioned persons.

2. Before the sale of goods/provision of service on the platform, sign an agreement with the vendors/service providers to preclude deals between the vendors/service provides and customers that can be associated with fraud and/or unauthorized transaction. The breach of this provision will result in the termination of the Agreement without notice.
3. Make sure that the vendors'/service providers' names included in the POI (Point of Interaction – a system/device used by a cardholder to carry out a financial transaction) data are protected from third party use, to prevent an unlawful use of trademarks/tradenames, including an illegal use of corporate names by entities acting in bad faith. Control tools may include vendor / service provider name monitoring by means of special lists (if any);
4. In view of a vendor's/service provider's business activity, put in place a tool to estimate loss due to fraud/unlawful action (including trade in counterfeit goods / breach of intellectual rights).
5. Check and control POI (Point of Interaction – a system/device used by a cardholder to carry out a financial transaction) data and the vendors'/service providers' business activity to make sure that all transactions to the sale of goods/provision of service are carried out in line with the vendors'/service providers' jurisdiction and the code of ethics and standards.
6. Be aware of its responsibilities for all activities and deviations, responsibilities/obligations related to customer service, inter alia with regard to disputes/chargebacks/claims initiated by customers.
7. Provide the Bank with any transaction/vendor/service provider-related information and/or document immediately and/or within the term set by the Bank, or fully compensate the Bank for the loss/damage incurred due to non-submission/late submission of such information/document.
8. Control vendor(s)/service provider(s) to prevent them from carrying out activities (including sale of goods/provision of

service on the platform) prohibited by the Georgian legislation / the Bank's policy / as well as rules/policies/regulations of international payment networks (VISA International and Mastercard Worldwide). The Merchant will be fully responsible for any such violation detected by the Bank (including for the compensation of damage, if any). Furthermore, the Merchant will be fully responsible for the quality of goods sold/services provided, any information supplied to customers, as well as the goods/service-related content published on the platform.

9. In case of chargebacks, fully refund the customer the disputed amount (the Merchant shall bear full responsibility for any customer complaint/claim/chargeback related to the purchase of goods/service on/via the platform). Furthermore, the Merchant shall keep documents/information related to the disputed transaction (invoice(s), transfer and acceptance document(s), other document(s) related to goods sold/service rendered, software entries, etc.) for 180 (one hundred and eighty) days and provide them to the Bank upon request (immediately and/or within the term and in a form required by the Bank).