Key Terms and Conditions of the E-Commerce Agreement (hereinafter referred to as "Key Terms")

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;

1.2 The Bank will settle VISA and Mastercard transactions to the Merchant's account, as envisaged herein;

1.3 Terms and conditions of the Agreement are additionally regulated by the Standard Terms and Conditions of the E-Commerce Agreement (hereinafter referred to as "Standard Terms" attached hereto) and relevant annexes to Key Terms and/or Standard Terms and/or to any application signed by the Merchant, whereby he/she/it accepts this Agreement (Key Terms and Standard Terms) (hereinafter referred to as the "Application") and the annexes hereto that are attached to the aforementioned documents and/or will be signed/agreed by and between the Parties in the future and represent an integral part hereof;

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.

1.5 The Parties agree that if the Bank's amendments/additions to any provision envisaged in the Agreement and/or in any annex and/or in any application and/or published on the Bank Website are favourable for the Merchant, the Bank is not obliged to inform the Merchant thereon in advance.

1.6 Any notification between the Parties shall be made in writing or in any other way envisaged in this Agreement. Written notifications shall be delivered to the Party's address last known to the other Party (the addresser). For notifications, the Bank can also use other communication channels (including, electronic, digital, telephone, etc.);

1.6.1 The Parties agree that any electronic notification sent to the email address provided by the Merchant and indicated (a) in this Agreement and/or (b) in any document/application presented/submitted to the Bank/signed by the Merchant and/or (c) in any public source shall be deemed officially delivered to the Merchant;

1.6.2 If a notification is sent to the Party by email, its receipt/delivery to the Party shall be confirmed by an extract from the respective device and/or a confirmation received by means of the device. The Merchant agrees that the notification sent to an email address indicated in Sub-Paragraph 1.6.1 of this Agreement shall be deemed delivered if its receipt or delivery to the Party is confirmed by an extract from the respective equipment and or by a confirmation message received by means of the device;

1.6.3 A notification shall be deemed received/delivered even if it is returned to the sender because the recipient's address does not exist or the addressee refused to accept or evaded the notification;

1.6.4 The notification shall be likewise deemed received/delivered if the act of sending and delivery complies with any form and means of information exchange envisaged by the legislation.

1.7 All annexes and agreements on amendments and additions hereto shall be deemed an integral part hereof;

1.8 Issues not covered in the Agreement shall be governed by the effective law of Georgia;

1.9 Any disputes and conflicts between the Parties shall be resolved through negotiations. If the Parties cannot reach an agreement, the dispute shall be taken to the court of law for discussion and final resolution. The Parties agree that pursuant to Article 268.1^1 of the Civil Procedure Code of Georgia, upon the satisfaction of the Bank's claim related to the dispute arising out of the Agreement, the judgment made by the court of first instance shall be subject to immediate execution;

1.10 In case of any discrepancy between this Agreement and previous agreements signed by the Parties on the Subject Matter hereof, this Agreement shall take precedence;

1.11 Voidance and/or invalidation of any part hereof shall not result in the voidance and/or invalidation of the entire Agreement.

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.

Standard Terms and Conditions of the E-Commerce Agreement (hereinafter referred to as "Standard Terms")

1. Definition of terms used in the Agreement

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:

"**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;

"**Transaction**" – a payment operation involving authorization and settlement;

"**Card**" – an international payment card from VISA or Mastercard;

"**Cardholder**" (Client") – a person using a payment card or a digital wallet under a relevant agreement concluded with the issuer;

"**Batch**" – multiple transactions performed within 24 hours, which an e-commerce gateway transmits to the processor;

"**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;

"**Fee**" – a charge for contractual services paid by the Merchant to the Bank according to the rules envisaged in the Agreement and tariffs set out in the Application signed by the Merchant or published on the Bank Website;

"**Upfront Fee**" – an amount drawn by the Bank from the Merchant's account(s) in advance;

"**Top-up Fee**" – an amount calculated as follows: the Merchant's per-transaction service fees collected during an accounting month are summed up at the start of the following month. If the sum of the fees is less than the amount indicated in the Top-Up Fee box, the difference will be drawn by direct debit from any account of the Merchant in the month following the accounting month, to which the Merchant hereby agrees. The Parties agree that transaction fees accrued in the accounting month but debited in the following month are not assigned to the accounting month;

"**Deduction**" – drawing funds from the Merchant's bank account(s) to settle liabilities in compliance with the Agreement;

"**Inquest**" – collection and clarification of information by the Bank if a problem arises in connection with the Agreement;

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

"**Insurance Reserve**" – funds envisaged herein that are transferred by the Merchant to the Bank and/or deducted by the Bank from the settled transaction proceeds before they are credited to the Merchant's accounts. The Insurance Reserve is deposited into an intrabank account;

"Required Balance of the Insurance Reserve" – the minimum balance of insurance reserve defined by the Bank under the Agreement;

"**Reversal**" – a refund of the transaction amount to the client initiated by the Merchant if the client returns goods or rejects the service;

"**Business Day**" – a calendar day except any Saturday, any Sunday and any public holidays envisaged by the law of Georgia (from 10:00 am to 6:00 pm);

"**Deal/Transaction**" – a deal between the Merchant and the client aimed at the purchase of goods/ services, whereby payments are made using payment cards and the online shopping system;

"**Online Shopping System**" – application software and hardware operated by the Merchant that enable the Merchant to transmit goods/services data to the website and make deals;

"**Deal amount**" – funds payable to the Merchant for goods/services purchased by the client in compliance with deals and agreements concluded;

"**Good/Services**" - Goods/services sold by the Merchant online;

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

"**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.

"**Digital Wallet**" – a software-based system that stores payment card tokens and allows accepting payments for e-commerce transactions and at POS terminals. Payments carried out by means of a digital wallet are subject to the same terms and conditions as card payments envisaged in the Agreement.

„Pre-authorization" – a temporary hold placed on the transaction amount until full or partial capture or abortion of the transaction by the Merchant. Unless the Merchant finalizes the transaction and captures the amount within 30 (thirty) days of pre-authorization, the hold will expire.

2. Rights and Obligations of the Bank

2.1 In line with the Agreement, the Bank undertakes to:

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;

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;

2.1.3 At the Merchant's request, supply the Merchant with business transaction reports via e-mail or fax;

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.

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.

2.2 Under the Agreement, the Bank may:

2.2.1 Draw the following amounts from the Merchant's account(s) by direct debit:

1) Bank fees;
2) Amounts subject to reversal;
3) Chargebacks - amounts of disputed transactions and/or transactions that have been declared fraudulent by the card issuer;
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;

2.2.2 Draw funds from transaction amounts by direct debit in order to maintain the Required Balance of the Insurance Reserve;

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

2.2.4 If, within one calendar month, the total amount and/or number of chargebacks reaches 1% (one percent) of the total amount and/or number of transactions or if the number and/or amount of transactions grows sharply, suspend card services and settlements for the Merchant until the causes are identified (through inspection);

2.2.5 Require from the Merchant all necessary information and documents in the event of a chargeback as well as any suspicious and/or illegal transaction;

2.2.6 Suspend daily (24-hour) authorization of transactions if the Merchant defaults on the Bank's requirements related to the fulfilment of his/her/its Insurance Reserve obligations;

2.2.7 Suspend daily (24-hour) authorization of transactions in the ongoing month if in the previous month the Merchant has exceeded his/her/its online shopping transaction limits set out in this Application/ on the Bank Website;

2.2.8 Deduct the necessary funds by direct debit from the Merchant's transaction proceeds and/or any accounts(s) held by the Merchant with the Bank if the Required Balance of the Insurance Reserve is not sufficient to settle the Merchant's liabilities to the Bank arising out of Key Terms and Standard Terms. In the absence of transactions and/or account balance(s), the Merchant is obliged to forthwith fulfil his/her/its obligations upon the Bank's notice;

2.2.9 Without seeking the Merchant's further approval, open for the Merchant a payment (current/checking, card, sales, other similar accounts) and/or a Call Deposit account in any currency if the Bank finds out that the Merchant does not have such an account and/or it is necessary to open

such an account additionally (for fulfiling obligations hereunder, for performing transfers in a currency different from the currency of the settlement account(s), etc.). In this case, the Agreement and/or the Application shall be deemed the Merchant's application for opening a relevant account;

2.2.10 Deduct the Upfront Fee amount indicated in the Application/on the Bank Website from the Merchant's account(s) upon the signature of the Agreement/Application / upon the receipt of the Merchant's notification (request/ consent) via remote channel (including email and internet banking) regarding the use of any service envisaged by this Agreement. If the total fee collected from the Merchant's sales in the previous month exceeds the Upfront Fee, the latter will be returned in full to the Merchant's account. However, if the total fee collected from the Merchant's sales in the previous month is less than the Upfront Fee, respective fees will be drawn from the Merchant's account(s) in compliance with rules set forth herein;

2.2.11 If the Agreement is terminated, not return the upfront fee to the Merchant, regardless of the reason for termination;

2.2.12 If the Merchant captures the transaction after 30 (thirty) days from pre-authorization, the amount captured behind the time will be drawn from the Merchant's account(s) without the Merchant's further consent.

2.2.13 Due to the circumstances revealed as a result of the Bank's monitoring, unilaterally increase the limit(s) defined for the Company under the Application/on the Bank's web-site at any time without giving a notice to the Company/securing the Company's prior approval.

2.3 Although the Insurance Reserve percentage is specified in the Application/ on the Bank Website, the Bank can increase or decrease the percentage at any time at its own discretion. The revision must be based on the Merchant's chargeback and reversal indicators and amounts, the status of the Merchant's accounts, the volume of transactions and other key factors and standards;

2.4 The Bank has the right to suspend settlements for the Merchant and/or terminate the Agreement if there are material circumstances that may inflict a loss on or cause reputational damage to VISA and/or Mastercard Payment Systems.

2.5 If the Parties agree on charge(s)/tariff(s) other/lower than the Bank's standard charge(s)/tariff(s) for the service(s) under the Agreement provided the Company gives precedence to TBC Bank JSC's ecommerce service in accepting card payments during the validity period of the Agreement, the Bank is entitled to unilaterally increase the different/lower charge(s)/tariff(s) approved for the Company as soon as the Company breaches the term stipulated herein.

3. Rights and Obligations of the Merchant

3.1 Under the Agreement, the Merchant shall:

3.1.1 Open a current account with TBC Bank JSC (unless he/she/it already has one), where to transfer funds under the Agreement;

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;

3.1.3 Sell goods/services via online store in line with his/her/its field of business;

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.

3.1.5 Report to the Bank in writing any changes in his/her/its contact details (legal/physical address, bank details, telephone number, fax number, e-mail address), as well as in his/her/its status (including, legal status, field of business, liquidation, bankruptcy) as soon as these changes are put into effect;

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

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;

3.1.8 Ensure that the Bank has free access to all Internet and/or other information resources which the Merchant uses for the sale of goods/services;

3.1.9 Not perform a transaction (not accept a payment) unless it is directly related to the sale of goods/services offered by the Merchant to clients;

3.1.10 Not take part in transactions/fictitious transactions (without rendering a service to the client(s)) that are directly or indirectly related to money laundering;

3.1.11 Not submit a transaction document(s) (whether in a paper and/or electronic form), which the Merchant knows or should know is/are fake or has/have not been authorized by the Cardholder;

3.1.12 If the fees set by the Bank are not paid in full and/or in due time, ensure that all of the Merchant's outstanding payments/charges are duly settled within 10 (ten) calendar days of the Bank's respective notice. Otherwise, the Bank has the right to suspend any service(s) (including, the E-Commerce service) envisaged by the Agreement and/or annexes hereto, and furthermore, to terminate the service(s) (including, the E-Commerce Service) unless all of the liabilities are fully satisfied within 30 (thirty) calendar days of the suspension of the service(s);

3.1.13 Check all transactions performed via TPAY QR on TPAY WEB and/or in the mobile application;

3.1.14 Not require the client to post payment card details (card number, expiry date, etc.) to the Merchant's website; not save payment card details and/or disclose/transfer them to any third

party (except when directly required by the law); strictly comply with security standards for payment card transactions.

3.1.15 Follow the customer confidentiality policy.

3.1.16 Keep and maintain throughout the validity period of this Agreement relevant equipment, machinery and/or other means (including personnel qualification enhancement tools, internal control tools and other technical equipment) in order to ensure full compliance with information security/confidentiality standards and legislative requirements.

3.1.17 Display the transaction amount to the client before the transaction is performed.

3.1.18 Not refuse the client access to services envisaged herein for the purchase of goods/services unless the Merchant finds the transaction suspicious.

3.1.19 Capture the transaction amount no later than 30 (thirty) days from pre-authorization.

3.2. In compliance with the provisions of the Agreement, the Merchant is obliged to ensure that:

3.2.1 Payment transactions accepted by the Merchant feature all relevant card transaction data, the Merchant's activities comply with MCC (Merchant Category Code) assigned to him/her/it by TBC Bank JSC; the Merchant uses for its online transactions the website that is indicated in the Merchant's documents submitted to the Bank;

3.2.2 If the Merchant violates his/her/its obligations set forth in Paragraph 3.2.1 hereof, he/she/it pays the Bank a penalty of 25 000 USD for each event of violation;

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

3.2.4 The transactions are not subject to additional charges;

3.2.5 The Merchant does not accept any payment unless the purpose of the transaction is the sale of offered goods/services;

3.2.6 The Merchant is held responsible for the actions of his/her/its employees during their employment period;

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);

3.2.8 Goods/services are not exported to countries that are subject to legal and/or export restrictions;

3.2.9 A credit entry is not posted without a debit entry for the same transaction;

3.2.10 The Merchant performs all his/her/its obligations fully and properly;

3.3. The Merchant has the right to:

3.3.1. Receive from the Bank additional consultations and explanations/definitions regarding card transactions;

3.3.2. Carry out reversals;

3.3.3. Receive statements on its transactions.

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.

4. Responsibilities of the Parties

4.1. If the Parties default on their obligations set forth in the Agreement or the obligations are not duly and completely satisfied, the Parties shall be held responsible in compliance with the effective law of Georgia and the provisions of agreements concluded by and between them;

4.2. If the Merchant defaults on his/her/its obligations set forth in the Agreement or the obligations are not duly and completely satisfied, he/she/it shall compensate the Bank for direct or indirect losses whether inflicted intentionally or due to neglect;

4.3. The Bank's responsibility to pay damages arising out of or in relation to the Agreement is only limited to a direct and intentional damage. Therefore, the Merchant acknowledges that he/she/it will not have the right to make any claim against the Bank if the latter causes damage to the Merchant due to neglect, which includes reputational damage, loss of interest, etc.;

4.4. The Bank shall not be held responsible for payment errors due to incorrect banking details supplied by the Merchant or due to the Merchant's delay to report changes in banking details;

4.5. The Bank shall not be held responsible for the damage brought to clients or third parties due to the Merchant's default on his/her/its liabilities in any deal;
4.6. The Merchant shall be held responsible for the quality of goods/services offered for sale, as well as for the content of any information he/she/it provides to clients, including selling details displayed on the Merchant's website. The Merchant is likewise obliged to delete immediately any information about the Bank published on his/her/its website if required so by the Bank;
4.7. The Merchant shall be fully obliged to refund the amounts deducted/ to be deducted in compliance with the Agreement and/or the possible damage resulting from the deduction;
4.8. The Bank shall not be held liable to refund amounts deducted in compliance with the Agreement;
4.9 The Bank shall not be held responsible for the consequences of accepting notifications and/or documents sent to the Bank from the Merchant's addresses/accounts (email, internet banking) by a third party, and of its (the Bank's) subsequent actions.
4.10 The Bank shall not be held responsible for any damage/loss caused by a third party action(s) (including third party modifications made to the Merchant's website, application or any component thereof or authorized or unauthorized (including fraudulent) third party access thereto).

5. Force Majeure and Restriction of Obligations

5.1. The Parties are released from contractual obligations if non-fulfilment thereof is due to force majeure events ("Force-Majeure");
5.2. For the purpose of this provision, Force Majeure refers to unavoidable circumstances beyond the control of the Parties that do not depend on the Parties' actions or inactivity.

6. Validity Term, Amendment and Termination of the Agreement

6.1. This Agreement shall enter into effect immediately after the Bank confirms the receipt of the Application or receives the Merchant's notification (request/consent) via remote channel (including email and internet banking) regarding the use of any service(s) envisaged in this Agreement, and shall remain in force indefinitely;
6.2. The Merchant may terminate any or all services envisaged hereunder by giving the Bank 15 (fifteen) calendar days' written notice. In this case, the Merchant shall pay the Bank all fees and other charges related to the service(s) in question within 5 (five) calendar days of submitting a service termination notice to the Bank;
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;
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;
6.5. The Bank can exercise its right(s) set forth in Paragraphs 2.2, 2.3 and/or 2.4 of these Standard Terms for 180 (one hundred and eighty) days from the termination of the Agreement.

7. Confidentiality

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;

7.2. If the breach of disclosure by any of the Parties brings damage to the other Party or to third parties, the breaching Party shall pay the damages.

8. Other Terms

8.1. The Parties declare that the term of obligations undertaken by the Merchant and described in Paragraphs 3.1 and 3.2 of these Standard Terms shall begin from the moment transaction details are posted to the transaction archive (Authorization History). Batch data shall serve as evidence to testify to the deadline of the obligation(s).

Annex #1

Rules/conditions set out in the Annex are binding on companies that use e-commerce or TBC E-commerce gateway to accept payments:

1. The website must display the Merchant's full name and address clearly and prominently;
2. The website must indicate the Merchant's telephone number and email address, through which clients will be able to receive any information regarding current payments;
3. The website must provide full and clear description of the goods or services as well as display terms and procedures for the purchase of goods/services, order cancellation or refund. These details must be communicated to the client before the purchase of goods/services in order to prevent confusion, complaints and disputes;
4. Registered trademark logos of JSC TBC Bank, VISA and Mastercard must be displayed prominently, without any modifications;
5. As the client may be a non-resident / a foreign citizen, the website must also provide a foreign currency equivalent of the price of goods/ services;
6. Goods/service delivery terms and the related information (delivery time, price, exceptions, etc.) must be provided in detail;
7. Upon the delivery of goods/services, a transfer and acceptance report indicating the receiving party's name shall be filled out and signed by both parties;
8. The following documents must be published on the website and the client must agree to them before making a purchase:
• Confidentiality policy;
• Transaction security policy;
• Payment policy;
• Legislative compliance policy;
9. The website must feature the Merchant's DBA (the trade name) before the payment is completed. DBA will appear on the client's statement.
10. When a transaction is carried out, the cardholder data (name, address, telephone) must be necessarily indicated on the website and the information must be provided to the Bank upon the Bank's request in the course of 6 months from the transaction date.

Annex #2

This Annex regulates in-store payments via TPAY QR.

TPAY payment service terms and conditions for brick-and-mortar stores (physical Merchants):

1. Administrator rights and admission parameters on the TPAY platform will be assigned to the Director of the store. His/her access to the platform will be activated on his/her telephone number indicated in the Application submitted to the Bank;
2. The Merchant's Administrator will manage access levels to the Merchant's management panel on the TPAY platform;
3. Payments will be accepted by the Merchant's Administrator and/or a person(s) delegated thereto by the Administrator;
4. If payments are accepted through a mobile terminal (a printed QR code and/or the mobile application), the Merchant's Administrator and/or a person(s) delegated thereto by the Administrator shall not hand over the mobile terminal(s) to a third party/ies and/or allow third party access thereto;
5. If payments are accepted through a printed mobile terminal, the payment status will be received/checked by means of an SMS titled TBCSMS sent to the telephone number of the Merchant's Administrator and/or of the person(s) delegated by the Merchant's Administrator and/or by means of the TPAY platform/ TPAY application.

Annex #3

This Annex regulates TBC E-commerce payment terms and conditions for online stores (online Merchants):

1. Administrator rights and admission parameters on the TBC E-commerce platform as well as internet banking user rights must be assigned to the Director of the online store.
2. The Merchant's Administrator and users authorized thereto by the Company Administrator will have access to the website's TBC E-commerce integration parameters.
3. The Merchant's Administrator will manage access levels to the Merchant's management panel on the TBC E-commerce platform.

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.

Annex #5

This Annex regulates the relationship between the Company and the Bank when the Company is using the Split feature that means the splitting of the transaction amount on a pro-rata basis as set by the Company when the Customer(s) buy(s) goods/services via the e-commerce channel and the Bank's transferring the amount to the account(s) of the Company and the Bank Customer(s) (an entrepreneur/taxpayer natural person and/or a legal person/a company), holding an account at the Bank with which the Company cooperates in the process of provision of goods/services to the Customer) (hereinafter the Company Partner).

1. General process of using the Split feature is carried out according to the following scheme:
1.1. Based on the Company's relevant application/request, the Bank activates the Split feature for the Company. Besides, for taking a decision on activating the Split feature for the Company, the Bank is authorized to request the Company the submission of any additional information and/or documents. The Bank reviews the Company's application and in case of taking a positive decision, starts the provision of the service to the Company with the Split feature, in particular: 1.1.1. When the Customer performs the payment transaction of the price of goods/services via an E-Commerce channel, the Company shares with the Bank the information as to how to split the transaction amount (price of goods/services) between the Company and the Company Partner and the account number of the Company Partner whereto the Bank transfers a part of the transaction amount. Based on the mentioned information, the Bank posts/transfers the transaction amount (according to the tariff agreed/set between the Bank and the Company, by deducting the Bank fee (if any)) to the account(s) of the Company and the Company Partner, on a pro-rata basis as set by the Company, besides, the total transaction amount transferred to the account(s) of the Company and the Company Partner (including the Bank fee (if any)) must correspond to the price of goods/services bought by the Customer.
1.2. The Company is liable to:
1.2.1. Control the Company's partner(s) to prevent it/them from carrying out such an activity (including sales of such goods/services) that is prohibited by the Georgian law/the Bank's policy (full responsibility for any such event of breach (including the compensation for damages (if any) detected by the Bank lies with the Company);
1.2.2. Possess (and if necessary, supply the Bank upon request) the information about the Company's partner(s) (type of activity, business model, status, any change to the type of activity and/or other information);
1.2.3. Immediately supply the Bank the information whether or not the Company replaces/adds partner(s) and/or the type of activity of the Company's partner(s) differs from the activity defined at the time of the Split feature activation; In such cases, only if receiving a positive answer from the Bank it will become possible to consider the person the Company's partner for the purposes of using the Split feature;
1.2.4. Assume responsibility for the correctness of all information (including, the account number(s) of the Company's partners, amount to be transferred to the Company's partner(s), information on change/addition to the Company's Partner(s), etc.) and sharing the information with the Bank that it transfersto the latter within the use of the Split feature;
1.2.5. If the Customer claims against the transaction, compensate for the claimed amount in full and not only for the part that was transferred to it within the use of the Split feature); Besides, the Company is liable to keep the documents/information related to the claimed transaction (invoice(s), Transfer and Acceptance Certificate(s), other document(s) related to sold goods/provided service, program records,

etc.) for 180 (one hundred and eighty) days and supply the Bank upon request in the form/under the procedure/within the term set by the latter (besides, the Company's liability for supplying the Bank any information/document/report in the form, under the procedure/within the term set by the latter, applies to any transaction performed within the use of the Split feature).

2. The detailed description/procedures/terms of the use of the Split feature are published on the Bank's website: https://tbcpayments.ge/details/ecom/tbc.

3. The Bank represents and the Company unconditionally confirms that the Bank is not liable (completely refuses to bear responsibility) to control the taxation of the transaction amount(s) transferred to the Company and the Company Partner(s) within the Company's use of the Split feature in line with the tax legislation requirements (if necessary). Besides, the Company is liable not to take such actions that are related to tax fraud / facilitation of tax evasion (directly or indirectly) in any form whatsoever.

4. The Company is entitled to request the deactivation of the Split feature, by sending a notification on the deactivation to the Bank (in any form of the notification under the E-Commerce Agreement signed between the Bank and the Company/confirmed by the Company (including, electronically)). On the day of receivingthe notification, the Bank ensures the deactivation of the Split feature.

5. This Annex is an essential part of the E-Commerce Agreement signed between the Bank and the Company/ confirmed by the Company (including electronically) and all terms/articles/paragraphs/provisions of the mentioned Agreement apply hereto.

Annex #6

This Annex regulates the Company's (Companies') acceptance of online payments through direct integration with VISA's payment service provider CyberSource:

- CyberSource is a payment platform that enables online payment processing and payment card settlement through different methods and channels.
- CyberSource will enable the Company to accept online payments through direct integration with VISA CyberSource, meaning that the Company will have its own user account with CyberSource, in which to manage oline card payments and transactions).
- If the Company is willing to use VISA's CyberSource for accepting and managing online payments, upon its (the Company's) request, the Bank will support its integration with CyberSource and enable processing of transactions/settlement for the Company, which will be carried out as follows: the Company will directly access VISA CyberSource through API integration (API - an application programming interface that enables information transfer between two platforms, serves as a medium between a company and a user, and also allows connection and information exchange between companies); VISA will transfer the transaction data to the processor (UFC), which will forward the data to the Bank.
- Through CyberSource integration, the Company will be able to make use of the accomplished ecommerce payment gateway by selecting "Bank transaction processing via CyberSource" in the menu. In this case, the Company must get registered with the Bank (by following the Bank's procedure for registering companies in the e-commerce business customer database) and then the Bank will register the Company on the CyberSource platform, after which the Company will be enabled to accept payments.
- The Company hereby agrees that during its registration on the CyberSource platform carried out by the Bank, the Bank will transfer the Company's information to CyberSource (its trade name, address, contact details; information about its authorized representative(s) and/or employee(s) and/or contact person(s) (including their personal data: name, surname, email address and mobile phone number). The Company hereby confirms that it has to obtain its employee's and/or representative's and/or contact person's consent over processing their data envisaged herein, before transferring the data to the Bank. Furthermore, immediately upon the Bank's request but no later than the 2 nd business day therefrom, the Company shall submit to the Bank a consent form for data processing signed/certified by its employee and/or representative and/or contact person.
- To enable the Company to process transactions on its (the Company's) website, the Bank will assign a unique merchant identification number (Merchant ID) to the Company and set up for it a payment configuration, after which the Bank will receive an encryption key (for payment completion and secure encryption during technical integration) and 3D Secure settings (a mandatory security protocol on card payments) and share them with the Company.
- User credentials will be set up for the Company on the CyberSource platform, with which the Company will be able to log into the platform and manage (validate/cancel/export, etc.) transactions.
- To have access to the full CyberSource payment portfolio, the company may accept payments on its own via predesigned websites integrated with CyberSource. To do so, the Company must log into the readymade website platform, indicate CyberSource in the field for payments and enter the encryption key / 3D settings provided to it by the Bank.
- CyberSource enables the Bank to manage the Company's payments (view / manage / report, etc. transactions).

- The Company is aware and confirms that if the Company integrates CyberSource directly through the International Payment System VISA and VISA cancels or suspends the Company's access to CyberSource services (on any grounds whatsoever), the Bank will not be responsible for the consequences of cancellation and/or suspension. Furthermore, if VISA's forthcoming cancellation and/or suspension of services under this Annex comes to the Bank's notice in advance, the Bank will immediately notify the Company thereof in a form envisaged in this Agreement. The Bank is entitled to unilaterally limit/restrict the Company's access to CyberSource services anytime, without prior notice, in order to ensure that the legislative requirements are met and/or the Company's obligations under the Agreement and/or any Annex thereto are satisfied and/or the Company's financial problems are prevented. In this case, the Bank will not be responsible for the consequences of / for the damage/loss (if any) caused by the cancellation and/or suspension.
- A detailed description and terms and conditions of services envisaged in this Annex are provided on the Bank's website: https://www.tbcbank.ge/web/en/web/guest/cybersource

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).