TBC Bank E-Commerce

Key Terms and Conditions of the E-Commerce Agreement

Tbilisi ___ _____

TBC Bank JSC (hereinafter "the Bank"), represented by ------- ----------, on the one hand, and -------- ---------- (hereinafter "the Company/Sub-Acquirer"), represented by ------- ----------, on the other hand, hereby enter into this E-Commerce Agreement and agree on the following:

1. **Subject Matter of the Agreement and Definition of Terms**

1.1 The Company (an entrepreneur/ individual taxpayer and/or a legal entity/ organizational entity) shall ensure that Visa, Mastercard and American Express (Amex) payments are accepted for goods sold/services provided by the Merchant through TBC E-commerce and/or TPAY QR and/or GEOPAY as payment gateways, while the Bank shall settle VISA, Mastercard and American Express (Amex) payments for goods sold/services provided by the Merchant.

1.2. The definitions of terms and rules provided in the Agreement are compliant with the rules of international payment systems (payment network processors) VISA International, Mastercard Worldwide and American Express (Amex). Furthermore, the Contracting Parties agree that during the payment for goods (items) / service(s) using current/call deposit account(s), rules envisaged by the Bank's internal policy / procedure(s) / standard(s) and the Law of Georgia shall be given precedence, which does not preclude the Bank from being guided by the rules / requirements / terms and conditions / provisions envisaged by this Agreement / the International Payment Systems.

"**Authorization**" – for the purposes of this Agreement: a procedure whereby the availability of the necessary amount is checked in the card account and the amount is placed on 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, Mastercard or American Express (Amex);

"**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**" – according to the rules of VISA International, Mastercard Worldwide and American Express (Amex) and the laws of Georgia, 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 transaction); If the disputed transaction(s) was/were carried out using current account(s), the chargeback procedure differs from the one applicable to disputed card transaction(s) and is regulated by/follows the rules envisaged by the Law of Georgia and the Bank's internal policy/procedure(s)/standard(s), which does not preclude the Bank from being guided by the rules / requirements / terms and conditions / provisions envisaged by this Agreement / the International Payment Systems;

Account – a payment account (current account/card account/call deposit account) held by the Merchant/Client and used for the payment for goods (items)/service(s);

"**Fee**" – a charge for contractual services paid by the Company to the Bank according to the rules and tariffs set;

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

"**Top-up Fee**" – an amount calculated as follows: the Company'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 collected from the Company's transactions in the previous month 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 Company in the month following the accounting month, to which the Company 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 Company'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" – international payment systems (payment network processors) VISA and Mastercard;

"**Insurance Reserve"** – funds envisaged herein that are transferred by the Company to the Bank and/or withheld by the Bank from the Company's transaction proceeds before settlement (before being credited to the Company's accounts). The Insurance Reserve is deposited into the Bank's internal ("intrabank") account;

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

"**Reversal**" – a refund of the transaction amount to the client initiated by the Company 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**" – 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 internet-based transmission of goods/services data and making deals;

"**Deal amount**" – funds to be accepted by the Company as a compensation due to the Merchant for goods/services purchased by the client, based on deals made by and between the Merchant and the client and this Agreement;

"**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**" – transaction data generated electronically in the online shopping system upon card payment authorization in the card payment network. Electronic drafts are the basis for settlement between the Bank and the Company.

"**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 this Agreement.

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

Sub-acquiring – an activity whereby the Company enters into an agreement with and provides settlement for merchant(s)/vendor(s)/service provider(s) within the framework of this Agreement;

Sub-Acquirer – a company in charge of sub-acquiring;

Merchant – a trade and/or service facility that uses e-commerce services offered by the Sub-Acquirer;

2. Rights and Obligations of the Bank

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

2.1.1 Transfer transaction proceeds to the Company's account (an account provided by the Company to the Bank) in national currency based on Electronic Drafts and to the deadlines specified in the Application/on the Bank website (as per the applicable laws of Georgia);

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

2.1.3 At the Company's request, supply the Company with reports/information/documents related to the Merchant's transactions via e-mail or fax;

2.1.4 Notify the Company regarding a fraudulent transaction no later than the business day after the day on which 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 settled into the Company's account in compliance with the terms and conditions stipulated in the Agreement no later than the business day after the transaction date.

2.2 Under the Agreement, the Bank may:

2.2.1 Draw the following amounts from the Company's account(s) by direct debit (without the Company's further consent):

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 on the Bank due to an incident observed with the Company/due to charges against the Company;

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 If requested, provide the International Payment System with any information about the Company available to the Bank;

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 Company until the causes are identified (through inspection);

2.2.5 Require from the Company 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 Company 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 online shopping transaction limits set for the Merchant;

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

2.2.9 Without the Company's further approval, open for the Company 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 Company does not have such an account and/or it is necessary to open such an account additionally (for fulfilling 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 Company's application for opening a relevant account;

2.2.10 Deduct the Upfront Fee from the Company's account(s) for any service provided by the Company under this Agreement upon the receipt (signing) of a notification (request/ consent) via remote channel (including email and the internet bank). If the total fee collected from the Company's sales in the previous month exceeds the Upfront Fee, the latter will be returned in full to the Company's account. However, if the total fee collected from the Company's sales in the previous month is less than the Upfront Fee, respective fees will be drawn from the Company'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 Company, regardless of the reason for termination;

2.2.12 If the Merchant delays with capture beyond 30 (thirty) days from pre-authorization, the corresponding amount will be drawn from the Company's account(s) without the Company's further consent.

2.2.13 Due to the circumstances revealed as a result of the Bank's monitoring, as well as considering the frequency of the Merchant's transactions unilaterally increase/decrease the transaction limit(s) set for the Merchant under this Agreement (its Annexes) anytime without notifying the Company in advance / without 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 anytime at its own discretion. The revision must be based on the Company's chargeback and reversal indicators and amounts, the status of the Company's accounts, the volume of transactions and other key factors and standards;

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

2.5 The Bank has the right not to register, suspend or cancel any of the Company's Merchants if the Bank considers that the Merchant does not comply with the risk assessment standards established by the Bank;

2.6 The Bank has the right to set transaction limits for each Merchant of the Company in accordance with its risk assessment procedures. / by considering the frequency of Merchant's transactions and report the limits to the Company via a remote channel (the internet bank). Furthermore, the Bank reserves the right to unilaterally increase/decrease transaction limits for the Merchant anytime.

2.7 The Bank has the right to provide information and statements related to transactions performed under this Agreement to the Sub-Acquirer only, as well as complete settlements solely for the Sub-Acquirer, which rules out the Bank's obligation to transfer information to the Merchant and/or complete settlement for the Merchant directly;

2.8 The Bank shall be entitled to refuse services to the Sub-Acquirer if it does not have an active account(s) with the Bank;

2.9 To ensure that the Sub-Acquirer's financial obligations arising out of this Agreement are satisfied, the Bank shall have the right, without any further consent or permission from the Sub-Acquirer, to draw the corresponding amount from any account of the Sub-Acquirer by direct debit (without seeking the Sub-Acquirer's further consent thereto) anytime after such obligation occurs. If the funds thus drawn are in different currencies and conversion is required, TBC Bank JSC's commercial rate as of the time of debiting will apply.

2.10 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 Company

3.1 Under the Agreement, the Company shall:

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

3.1.2 After the Bank ensures that the payment gateway is integrated into the Merchant's website, ensure that the Merchant displays the information about card payment rules on the online store's website;

3.1.3 Control that the Merchant sells goods/services via online store in line with its (the Merchant's) 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 observed with/ charges laid against the Company;
- Any type of loss/damage caused to the Bank due to incorrect/inaccurate information about the Bank spread by the Company.

3.1.5 Report to the Bank in writing any changes in the Company's contact details (legal/physical address, bank details, telephone number, fax number, e-mail address), as well as any other change (including in 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 merchants with e-commerce websites, 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 has the right to deduct by direct debit the amounts indicated in Sub-Paragraph 3.1.4 hereof from the Company's Insurance Reserve and/or other accounts within 180 (one hundred and eighty) days of 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 Set the following restriction for the Merchant under the agreement with the Merchant:

3.1.9.1 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;

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

3.1.9.3 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;

3.1.9.4 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.

3.1.9.5 Follow the customer confidentiality policy.

3.1.9.6 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.

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

3.1.9.8 Not refuse the client access to services envisaged herein for the purchase of goods/services unless the transaction is found suspicious.

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

33.1.9.10 not refuse to accept payment by a card of a particular international payment scheme solely on the grounds that the card belongs to that particular international payment scheme, provided that the acceptance of such cards is contemplated by the agreement between the Bank and the Merchant;

3.1.9.11 not indicate, in any form, that a card of any international payment scheme is preferred over a card of another international payment scheme, or encourage a customer to use a card of a particular international payment scheme, except for providing information regarding a relevant offer made within the framework of a cashback, loyalty, discount or other incentive programme/campaign;

3.1.9.12 ensure that the policies and practices applicable within the scope of its activities do not provide for granting a card of any international payment scheme an advantage over, or otherwise treating it preferentially compared with, a card of another international payment scheme;

3.1.9.13 not impose any additional or different terms, conditions or restrictions on the use of a card of a particular international payment scheme that do not apply to cards of other international payment schemes;

3.1.9.14 not establish a minimum and/or maximum amount for a transaction made using a card of a particular international payment scheme, except for limits established by the Bank or where the relevant restriction applies equally and without discrimination to transactions made using cards of other international payment schemes;

3.1.9.16 include in the amount of a card transaction all taxes provided for under applicable law;

3.1.9.17 not conduct any transaction on behalf of another merchant and/or in consideration for goods supplied or services rendered by another merchant;

3.1.9.18 not split the amount of a single operation into multiple transactions for the purpose of avoiding the relevant authorisation requirement;

3.1.9.19 comply with the applicable requirements of the PCI Data Security Standard (PCI DSS);

3.1.9.20 in the event of unauthorised access to, disclosure or loss of customers' personal data, including card data, or any other security breach affecting such data, notify the Sub-acquirer thereof immediately, but no later than 72 hours after becoming aware of the relevant incident;

3.1.9.21 upon termination of the service agreement entered into with the Sub-acquirer, immediately ensure the removal of the marks of international payment schemes from all locations where they have been displayed.

3.1.10 If the fees set by the Bank are not paid in full and/or in due time, ensure that all of its 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);

3.1.11 Register and identify each Merchant in accordance with the regulations of the National Bank, payment systems and other regulators.

3.1.12 Strictly follow the requirements of regulators and payment systems.

3.1.13 The Company shall submit to the Bank full information or documentation about the Merchant required by the Bank during as well as after the registration of the Merchant.

3.1.14 Pay the Bank the annual fee of 3500 (three thousand and five hundred) EUR for the Company's registration as the Payment Facilitator in line with the requirements set by the Mastercard

international payment system, within 3 working days of signing the agreement and afterwards, before the expiration of each subsequent 12-calendar month period from signing the agreement.

3.1.15 Control the Merchant's transaction limits.

3.1.16 Provide the Bank with the details of the Merchant(s)'s transactions upon the Bank's request.

3.1.17 Provide the Bank with the information and documentation related to the transaction/Merchant immediately and/or within the period predetermined by the Bank. Otherwise, if any kind of damage occurs to the Bank due to non-submission of information/documentation to the Bank, the Sub-Acquirer shall be obliged to fully compensate the Bank for the mentioned damage.

3.1.18 If the Bank suffers damage due to chargebacks on any of the Merchant's transactions (including but not limited to third party claims/charges against the Bank, penalties/charges, etc.), the Sub-Acquirer shall be obliged to compensate the Bank for the damage caused within 3 (three) working days of the demand.

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

3.2.1 All of the Merchant's transactions feature all relevant card transaction data; the Merchant's activities are in line with MCC (Merchant Category Code) assigned to it by TBC Bank JSC; a Merchant uses for its online transactions the website that is indicated in the documents submitted by the Company to the Bank;

3.2.2 If the Company violates its obligations set forth in Paragraph 3.2.1 hereof, it pays the Bank a penalty of 25 000 USD for each event of violation;

3.2.3 The Merchant only uses the payment tools/gateway(s) mentioned herein for accepting payments for goods/services sold;

3.2.4 The Merchant(s) do(es) not charge any extra payment;

3.2.5 The Merchant(s) do(es) not accept any payment unless the purpose of the transaction is the sale of offered goods/services;

3.2.6 The Company is held responsible for the actions of its employees during their employment period;

3.2.7 It implements anti-money laundering restrictions and takes all relevant measures, acts in compliance with 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). Furthermore, by means of its agreement with the Merchant, will obligate each Merchant to put in place / take the measures set out herein and strictly adhere thereto.

3.2.8 The Merchant does not export goods/services 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 Company performs all of its obligations fully and properly;

3.2.11 ensure that its activities and those of the Merchants are conducted in full compliance with the rules, requirements, standards and procedures of the international payment schemes.

3.3. The Company has the right to:

3.3.1. Receive at the Bank additional consultations and explanations regarding card transactions;

3.3.2. Carry out reversals;

3.3.3. Receive statements on the Company's / Merchant(s)'s transactions.

3.3.4 Not to integrate a Merchant in its own system without the Bank's prior consent;

3.3.5 Upon the Bank's request, submit to the Bank a complete list of Merchants along with the information and/or documents related to their current activities;

3.3.6 Not to serve and/or immediately suspend provision of services to Merchants whose activities are:

3.3.6.1 pornography;

3.3.6.2 trade in unlicensed/unexcised products, including tobacco, alcoholic beverages, etc. (only in case of e-commerce)

3.3.6.3 internet retailing of tobacco products, tobacco accessories and/or devices intended for tobacco use, except for tobacco accessories and/or devices intended for tobacco use, which do not bear the trademark and/or name of the products

(goods) of persons involved in the tobacco industry (only in case of e-commerce);

3.3.6.4 dealers and manufacturers of ammunition and other unlicensed weapons;

3.3.6.5 unlicensed digital content (only in case of e-commerce)

3.3.6.6 replica "fake" products (only in case of e-commerce)

3.3.6.7 Forex/Binary/Options

3.3.6.8 prescription drugs (only in case of e-commerce)

3.3.6.9 online casinos and other gambling businesses (if there is no physical representation in Georgia);

3.3.6.10 other illegal activities, such as trafficking, prostitution, drug trade, etc.

3.3.6.11 trade in narcotic drugs, including so-called "soft drugs" and their devices.

3.3.7 If the Sub-Acquirer violates Sub-Paragraph 3.3.6 of this Agreement, the Bank shall be entitled to immediately suspend and/or terminate the validity of the agreement and demand from the Sub-Acquirer the payment of an indemnity in the amount of 10 000 GEL.

3.3.6.1 check-cashing and/or check-guarantee services (Check Cashing/Check Guarantee);

3.3.6.2 credit history and/or credit rating restoration services (Credit Restoration Services);

3.3.6.3 activities associated with persons and/or organisations identified by the U.S. Government as supporting terrorism and included on the relevant sanctions list maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC);

3.3.6.4 the production, distribution and/or sale of products that infringe the intellectual property rights of third parties (Sale of Infringing Products).

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 Company 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 Company 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 Company or due to the Company'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 Company's and/or the Merchant's default on their liabilities in any deal;

4.6. The Company/the Merchant shall be held responsible for the quality of goods/services offered for sale, as well as for the content of any information they provides to clients, including selling details displayed on the website. The Company 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 Company 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 Company' 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 Company's website, application or any component thereof or authorized or unauthorized (including fraudulent) third party access thereto).

4.11 The Company and the Merchant negotiate with each other agreement terms and conditions/provisions/penalty limits, etc, including those related to the sub-acquiring agreement, independently of the Bank. Therefore, the Bank shall not be held responsible for any consequences/damage/loss resulting from the mentioned agreement.

5. Force Majeure

5.1. The Parties to this Agreement shall not be held responsible for non-satisfaction of contractual obligations if delayed fulfilment or 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 are not related to the Parties' mistakes or negligence and are unforeseeable. These circumstances may have resulted from war, natural disasters, epidemic, quarantine, etc.

5.3 In force-majeure circumstances occur, the Party which is unable to meet its obligations shall forthwith notify the other Party in writing of the circumstances and the underlying causes. If the notifying Party does not receive the other Party's response, it shall continue to perform its contractual obligations at its own discretion, to an extent considered reasonable and possible and make an effort to find alternative ways unaffected by the force-majeure circumstances in order to meet its obligations.

5.4 If a force-majeure circumstance persists more than 1 (one) month, the other Party is entitled to terminate the Agreement by notifying the Party thereof.

6. Validity Term, Amendment and Termination of the Agreement

6.1. This Agreement shall enter into effect immediately upon signature by the Parties and remain in force indefinitely;

6.2. The Company may terminate any or all services envisaged hereunder by notifying the Bank thereof 15 (fifteen) calendar days in advance. In this case, the Company 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 anytime by giving the Company 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 has the right to make amendments/additions to the terms and conditions and features of the services(s) described herein and/or charges/tariffs/payments set for the Company/the Merchant under this Agreement / Annex(es) / by sending to the Company a notification via remote channels (the internet bank) 1 (one) month in advance. Furthermore, if the Bank makes amendments/additions to its charges / tariffs / payments, it may propose the Company and/or terminate the provision of any or several services envisaged by the Agreement or annexes hereto. The Company 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 Company. If the Company 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 Company hereunder. If the Company does not exercise its right to terminate the Agreement, the amendments/additions proposed by the Bank shall be deemed accepted by the Company and the provisions/tariffs/charges shall be amended as proposed. The Bank can effect amendments/additions that do not deteriorate the Company's position as soon as they are published on the website/communicated to the Company in a notification.

6.5. The Bank can exercise its right(s) set forth in Paragraphs 2.2, 2.3 and/or 2.4 of this Agreement for 180 (one hundred and eighty) days from the termination of the Agreement.

6.6 Any notification / agreement made by and between the Parties under this Agreement and/or Annex(es) hereto shall be in writing and/or sent via a remote channel (the internet bank). A written notification shall

be delivered to the Party's address last known to the sender. The Bank may also use other communication channels (including electronic, digital, telephone, etc.);

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 consent any information that directly or indirectly relates to the Agreement and is confidential. This obligation shall remain valid after the termination of this Agreement;

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

8. Provision about Sanctioned Persons

8.1 The Sub-Acquirer represents and warrants that:

8.1.1 At any time before the execution of this Agreement or during the validity period hereof, the Sub-Acquirer/the Merchant(s), their shareholders, management or the members of their executive/supervisory body, as well as the Sub-Acquirer's/the Merchant(s)'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:

8.1.1.1 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).

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

8.1.1.3 Have 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.

8.1.1.4 Have 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.

8.1.1.5 If the statement/representation made pursuant to Paragraph 8.1 is found untrue and the Sub-Acquirer's/Merchant(s)'s, activity qualifies as a breach/evasion of sanction and/or according to the Bank's assessment, the aforementioned fact exposes the Sub-Acquirer/Merchant(s), their shareholders, member(s) of their management or executive/supervisory board and/or their 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 8.1.1.1 hereof and take any and all measures set and/or required by the Authorized Person(s) and/or Entities/Bodies, inter alia, prevent the Sub-Acquirer/Merchant(s), from using/disposing of and managing any funds/assets.

9. **Resolution of Disputes**

9.1 Disputes arising out of this Agreement shall be resolved through negotiations. If the Parties fail to come to an agreement, they are entitled to apply to the court in line with the applicable laws of Georgia.

9.2 The Parties agree that if the dispute is taken to the court, the ruling of the first instance court in favour of the Bank shall be immediately enforceable pursuant to Article 268.1[1] of the Civil Procedure Code of Georgia.

10. Closing Provisions

10.1 The Parties declare that the term of obligations undertaken by the Company and described in Paragraphs 3.1 and 3.2 of the Agreement shall begin from the moment transaction details are posted to the transaction archive (Authorization History). Batch data shall serve as evidence based on which to establish the due date of the obligation(s).

10.2 Cases not covered in this Agreement shall be governed by the applicable regulations and norms estbalished under the Georgia law.

10.3 Any annex and/or amendment/addition hereto shall be deemed an integral part hereof.

10.4 Revocation of any part hereunder shall not result in the revocation/termination of the entire Agreement.

10.5 This Agreement shall be deemed an integral part of the Agreement on Banking Transactions made by and between the Bank and the Sub-Acquirer / validated by the Sub-Acquirer, meaning that this Agreement shall be fully subject to the effect of the Agreement on Banking Transactions.

10.6 This Agreement has been composed in Georgian in two identical counterparts with equal legal force, one copy for each.

The Bank
TBC Bank JSC
ID #----------
Address: ----------
Email: ----------

The Company/Sub-Acquirer

ID #----------
Address: ----------
Tel.: ----------
Email: ----------

Annex #1

Rules/conditions set out in Annex #1 herein are binding on the Company(ies)/the Merchants that use e-commerce or TBC E- commerce to accept payments:

1. The website must display the Company's full name and address clearly and prominently;
2. The website must indicate the Company'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, Mastercard and American Express (Amex) 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 Company's DBA (the trade name) before the payment is completed. The 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 Companies):

1. Administrator rights and admission parameters on the TPAY platform will be assigned to the Director of the Company. His/her access to the platform will be activated on his/her telephone number indicated in the Application which the Company submits to the Bank;
2. The Company's Administrator will manage access levels to the Company's management panel on the TPAY platform;
3. Payments will be accepted by the Company'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 mobile app), the Company'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 Company's Administrator and/or of the person(s) delegated by the Company'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 goods/services providers (Companies):

1. Administrator rights and admission parameters on the TBC E-commerce platform as well as internet banking user rights must be assigned to the Company Director.
2. The Company's Administrator and users authorized thereto by the Company Administrator will have access to the website's TBC E-commerce integration parameters.
3. The Company's Administrator will manage access levels to the Company'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 authoried 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 monitoring.
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 analazed as necessary for investigating an incident or an error.
5.11 Remote storage/ Cloud Service must not 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, which means the splitting of the transaction amount paid by a customer for goods/services purchased via ecommerce channel based on the ratio set by the Company and the Bank's settlement of the split amount into the account(s) of the Company and the Bank Client(s) (an entrepreneur/taxpayer natural person and/or a legal person/a company) who hold an account with the Bank and cooperate with the Company in the provision/delivery of goods/services to the customer) (hereinafter the Company Partner).

1.

1. The overall process of using the Split feature shall follow the scheme described below:

1.1. Based on the Company's relevant application/request, the Bank activates the Split feature for the Company. For taking a decision regarding the activation of the Split feature for the Company, the Bank is authorized to request from the Company the submission of any additional information and/or documents. The Bank reviews the Company's application and in case of a positive decision, starts to provide the Company payment splitting services, in particular:

1.1.1. When a customer pays the price of goods/services via E-Commerce channel, the Company submits to the Bank the ratio for splitting the transaction amount (price of goods/services) between the Company and the Company Partner, as well as the account number of the Company Partner, where to settle the Partner's share in the transaction amount. Based on the mentioned information, the Bank settles the transaction amount into the Company's and the Company Partner's respective accounts by applying the ratio set by the Company (and using the tariff agreed/set between the Bank and the Company, less the Bank's fee (if any)). The total transaction amount settled into the Company's and the Company Partner's accounts (including the Bank fee (if any)) must match 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 provide the Bank with 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. A person/entity will qualify as the Company's Partner under the splitting service based on the Bank's approval only;

1.2.4. Assume responsibility for the correctness/accuracy of the entire information submitted to the Bank under the splitting service (including the Company Partner's/Partners' account number(s), amounts due to the Company Partner(s), information about the Partners replaced/added, etc.), as well as for timely provision of the information to the Bank;

1.2.5. If a customer files a chargeback against the transaction, refund the claimed amount in full and not only the part settled into its account under the splitting service); Besides, the Company shall keep the documents/information related to the chargeback (invoice(s), Transfer and Acceptance Certificate(s), other document(s) related to sold goods/provided service, program records, etc.) for 12 (twelve) calendar months and supply them to the Bank upon request in the form/by the procedure/within the term set by the latter (the Company's obligation to provide the Bank with any information/document/report in the form, under

the procedure/within the term set by the latter, applies to any transaction performed under the splitting service).

2. The detailed description/procedures/terms of 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 receiving the notification, the Bank ensures the deactivation of the Split feature.
5. This Annex is an essential part of the E-Commerce Agreement signed by and between the Bank and the Company/ validated by the Company (including electronically) and all terms/articles/paragraphs/provisions of the mentioned Agreement apply hereto.

Annex #6

Policy against Bribery, Corruption and Facilitation of Tax Evasion

1. The parties represent and warrant as follows:
   1.1 Each party, their subsidiaries, parent companies, related entities will carry out their activities and engage in business relations in due manner and good faith and by adhering to high ethical standards. The parties have zero tolerance towards bribery, corruption, tax fraud, tax evasion and any other criminal activities and exercise permanent control over these issues.
   1.2 The parties and the related entities, the members of top management, authorized representatives, employees, other personnel of their subsidiaries and parent companies, shall not participate in actions that involve:
      1.2.1 the offer, receipt, delivery, issuance or request, directly or indirectly, of a gift, hospitality and other intangible benefits for the purpose of gaining a commercial, contractual, regulatory or personal advantage and/or encouragement or awarding for illegal and unethical action.
      1.2.2 Any form of facilitating /abetting corruption, tax fraud, tax evasion (whether direct or indirect);
   1.3 None of the parties or the related entities:

   1.3.1 Upon signing an agreement, has directly or indirectly paid, received, been involved in any deal, within which it has to pay or receive, any illegal and/or hidden fee, bribe and/or compensation.

   1.3.2 For signing an agreement, has taken any action aiming at, inter alia, artificial regulation of prices and/or creation of incompetitive environment and/or the exercise of influence over the actions of an authorized representative of a member of top management, employee, other personnel or the related party and/or the related company of one of the parties, and/or nor the aforementioned entities have threatened the property or reputation of another party and/or acted in bad faith to gain unfair business advantage and/or have been involved in a corruption activity in any other way.

   1.4 None of the parties is a public entity and acts on behalf of the latter. Both parties undertake to forthwith inform the other party regarding a change in this clause.

   1.5 None of the parties or the related parties have been either convicted for and/or accused of corruption, bribery, tax fraud,, tax evasion or facilitation thereof.

2. Violation of any of the aforementioned provisions may result in the termination of this Agreement, as well as any agreement already signed between the Parties. Furthermore, the aforementioned termination does not exclude holding the breaching Party and/or the member of its top management, its authorized representative, employee, other personnel or a party related to it responsible and applying relevant sanctions against any of them, as envisaged by the legislation. The Parties also confirm that acts committed by the Party's top management, authorized representative, other personnel or the related party and/or the related company shall not invoke the Party's responsibility unless committed on behalf or on the instruction of the Party.
3. The mentioned representations and warranties are valid until the full and proper execution of obligations assumed under this Agreement and/or any or all other existing agreement(s), regardless of full or partial termination of these agreement(s).

4. A party shall forthwith notify the other party in writing regarding any and all circumstance(s), which may contradict and/or result in the breach of these warranties; as well as regarding the commencement or occurrence of a circumstance/event that may threaten the full and proper execution of obligations assumed under the agreement(s). Depending on the gravity of violation of these warranties, for the purpose of inspection, the Bank will be authorized to require from the contracting party submission of reports and records.

Annex #7
Transaction Tariffs / Fees

The Sub-Acquirer will set the following tariffs/fees for each Merchant:

- ----------
- ----------
- ----------

Annex #8

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 SyberSpace, meaning that the Company will have its own user account with SyberSource, 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 e-commerce 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 2nd 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 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 #9

The Rules/Terms hereunder are binding on the Companies 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 Company 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, Mastercard Worldwide and American Express (Amex)). The Company will be fully responsible for any such violation detected by the Bank (including for the compensation of damage, if any). Furthermore, the Company 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 Company shall bear full responsibility for any customer complaint/claim/chargeback related to the purchase of goods/service on/via the platform). Furthermore, the Company 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 12 (twelve) calendar months and provide them to the Bank upon request (immediately and/or within the term and in a form required by the Bank).

Annex #10

This Annex regulates the Company's (Companies') acceptance of online payments through **Mastercard Payment Gateway System (MPGS)** integration:

- Mastercard Payment Gateway System (MPGS) is a Mastercard payment gateway that enables online payment processing through different methods and channels (hereinafter the "Payment Gateway"). The intellectual property holder on the Payment Gateway is Mastecard.
- MPGS /Payment Gateway will enable the Company to accept online payments and manage online payments and transactions on its own through MPGS/Payment Gateway integration.
- If the Company is willing to use MPGS/Payment Gateway for accepting online payments, upon its (the Company's) request, the Bank will support its integration with MPGS/Payment Gateway, while afterwards, the Bank will provide payment processing/settlement. The process will be implemented using an API (an application programming interface) that enables information transfer between two platforms and serves as a medium between a company and a user.
- In order to register with and use MPGS /Payment Gateway, the Company hereby agrees and authorizes the Bank to transfer to MPGS the Company's information (including its trade name, address and contact details), as well as the information / personal data of the Company's 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 represents and warrants that it will obtain its employee's (employees') and/or representative's (representatives') and/or contact person's (contact persons') consent to the processing of their data envisaged herein before the data processing is started / the data are transferred to the Bank. Furthermore, immediately upon the Bank's request but no later than the 2nd business day therefrom, the Company undertakes to submit to the Bank the aforementioned consent(s).
- The Company is aware and agrees that the Bank will also report to MPGS regarding the Company's activation or deactivation with MPGS/Payment Gateway.
- To enable the Company to handle transactions on its (the Company's) website, the Company will be assigned a unique identification number (Merchant ID) and will receive an encryption key (for facilitating payment processing and secure encryption during technical integration).
- User credentials will be set up for the Company on MPGS/Payment Gateway, with which the Company will be able to log into the platform (undergo authentication) and manage (validate/cancel/export, etc.) transactions.
- MPGS Payment Gateway enables the Bank to manage the Company's payments (view / manage / report, etc. transactions).
- The Company is aware and confirms that if the Company's direct integration with the MPGS/Payment Gateway, through the International Payment System Mastercard, if the Company's gateway integration/access thereto is cancelled and/or suspended, regardless of the reasons and/or the grounds, the Bank will not be responsible for the consequences of the cancellation/suspension. If Mastercard's forthcoming cancellation and/or suspension of the service 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.
- Furthermore, the Bank is entitled to unilaterally limit/restrict the Company's access to the Gateway Platform at any time, 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/avoided. 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.
- The Company is obliged to use the Gateway as per the Bank's instructions/Rules and solely for the purpose for which the Bank facilitated the Company's Gateway integration. The Company is prohibited from using the Payment Gateway for other purposes, as well as from making changes to / modifying / isolating the platform or any part thereof.
- It is prohibited to implement/run any process or intervention (including penetration testing, etc.) related to

the Payment Gateway without the Bank's prior approval.

- If any of these terms is/are breached, the Company shall be responsible for any damage/loss caused to the Bank.
- A detailed description and the terms & conditions of the service envisaged in this Annex are provided on the Bank's website: https://www.tbcbank.ge/web/en/web/guest/mpgs

The Bank
TBC Bank JSC
ID #----------
Address: ----------
Email: ----------

The Company/Sub-Acquirer

ID #----------
Address: ----------
Tel.: ----------
Email: ----------