Īpašie noteikumi maksājumu karšu pieņemšanai Luminor Phone POS

1. pielikums Karšu pieņemšanas noteikumiem

Papildus Noteikumiem šie Īpašie noteikumi karšu pieņemšanai Luminor Phone POS (turpmāk – "**Īpašie noteikumi**") tiek piemēroti Pušu savstarpējām attiecībām par Luminor Phone POS pakalpojuma sniegšanu, kā noteikts šajā 1. pielikumā. Ja 1. pielikuma noteikumi ir pretrunā Noteikumiem, priekšroka tiek dota šiem 1. pielikuma noteikumiem, ciktāl tos piemēro Luminor Phone POS pakalpojumam.

1. Šādiem terminiem ir turpmāk norādītā nozīme Īpašajos noteikumos:

   1.1. **Administrators** – Lietotājs, kam Komersants ir atļāvis administrēt Lietotāja tiesības izmantot Komersanta portālu.

   1.2. **Autentifikācijas līdzekļi** – elementi, kas Bankas noteiktajā kārtībā ļauj autentificēt personu un/vai pārbaudīt konkrēta maksāšanas līdzekļa lietošanas pamatotību, tostarp personalizēti autentifikācijas dati, piemēram, lietotāja (klienta) numurs, pieteikumvārds, kods, parole, tālruņa numurs, ierīces dati (piemēram, sērijas numurs, IMEI numurs), personas dati (piemēram, vārds, uzvārds, personas kods), tostarp biometriskie dati (piemēram, pirkstu nospiedumi, sejas digitālais attēls, varavīksnenes attēls, balss ieraksts utt.), kā arī elektroniskais paraksts (elektroniskie dati var būt jebkurš no iepriekš minētajiem elementiem un/vai citi elektroniskie dati), kvalificēts elektroniskais paraksts utt.

   1.3. **Komersanta akreditācijas dati** – informācija paroles iestatīšanai, lai piekļūtu Luminor Phone POS, kas tiek saņemta Pieteikumā norādītajā e-pastā.

   1.4. **Komersanta ierīce** – jebkura ierīce, kas izmanto lietotni jebkurā ar tuvā lauka sakaru iespējotā

Special Provisions for Luminor Phone POS Card Acceptance

Annex No 1 to Card Acceptance rules

In addition to other provisions of Rules these Special Provisions on Luminor Phone POS Card Acceptance (hereinafter – **Special Provisions**) shall apply to mutual relations between the Parties regarding the provision of Luminor Phone POS service as defined in this Annex 1. Should the provisions of Annex 1 herein fall in conflict with other provisions of the Rules, those of Annex 1 shall prevail, as far as applicable to the Luminor Phone POS service.

1. The following terms have the following meaning within Special Provisions:

   1.1. **Administrator** – User whom the Merchant has authorized to administer the Users' rights of usage of the Merchant Portal.

   1.2. **Authentication Instruments** – elements, which in accordance with the procedures of the Bank enable authentication of a person and/or verify the validity of use of a specific payment instrument, including personalized authentication data, for example, user (customer) number, login, code, password, phone number, data of the device (for example, serial number, IMEI number), personal data (for example, name, surname, personal code), including biometric data (for example, fingerprints, digital image of the face, iris image, voice recording, etc.), as well as electronic signature (electronic data may constitute any of the aforementioned elements and/or other electronic data), qualified electronic signature etc.

   1.3. **Merchant Credentials** – information to set a password to access to Luminor Phone POS is received in such email indicated in the Application

(NFC iespējotā) ierīcē ar operētājsistēmu Android 9+, kas sākotnēji tika piegādāta ar Android 8.versiju vai jaunāku versiju un ir reģistrēta Luminor Phone POS pakalpojuma lietošanai, izmantojot Komersanta akreditācijas datus.

1.5. **Komersanta portāls** - digitālais kanāls, ko iespējojis Komersants, lai veiktu konkrētas darbības, kas saistītas ar Luminor Phone POS pakalpojumu.

1.6. **Lietotājs** - fiziska persona, kurai Komersants atļauj lietot Komersanta ierīci un/vai Komersanta portālu.

1.7. **Luminor Phone POS pakalpojums** - Bankas pakalpojums maksājumu karšu pieņemšanai, izmantojot Luminor Phone POS lietotni, kas instalēta Komersanta ierīcē.

1.8. **Luminor Phone POS** - Google Play pieejamā lietotne.

1.9. **Noteikumi** – Karšu pieņemšanas noteikumi, kuru pielikums ir šie Īpašie noteikumi

1.10. **Parole** - parole, ko Komersants iestatījis Luminor Phone POS lietotnē, kas ļauj piekļūt Luminor Phone POS lietotnei.

2. Lai izmantotu Luminor Phone POS pakalpojumu, komersants saņem e-pasta ziņojumu, kas satur unikālo saiti, lai piekļūtu paroles iestatīšanas modulim, iestata personīgo paroli; lejupielādē lietotni (ja vēl tas nav izdarīts pirms šīs darbības); atver lejupielādēto Luminor Phone POS lietotni, ievada savus Komersanta akreditācijas datus un pieņem visas nepieciešamās atļaujas, kas jāiespējo darbam ar lietotni.

3. Komersanta ierīcei jābūt ar stabilu interneta pieslēgumu un NFC tehnoloģiju, kas pieejama un aktivizēta, lai izmantotu Luminor Phone POS pakalpojumu.

4. Komersants norāda e-pastu katrai ierīcei, ko Komersants plāno izmantot kā Komersanta ierīci, lietotnē Luminor Phone POS pakalpojuma izmantošanai un/vai Līgumā. Komersants var mainīt šo informāciju (pievienot/dzēst ierīci), nosūtot Bankai rakstisku paziņojumu, kas pēc formas un satura ir Bankai pieņemams. Banka izvērtē ierosinātās izmaiņas 3 (trīs) Darba dienu laikā. Ja Bankai izmaiņas ir pieņemamas, Komersanta rakstisks paziņojums tiek uzskatīts par Līguma sastāvdaļu un Banka veic nepieciešamās darbības

1.4. **Merchant Device** – any device that uses the application on any Near Field Communication-enabled (NFC-enabled) Android 9+ device, that was originally shipped with Android version 8 or higher and that is registered for the use of Luminor Phone POS service by using Merchant's Credentials.

1.5. **Merchant Portal** – a -digital channel enabling the Merchant to perform specific activities related to Luminor Phone POS service.

1.6. **User** – a natural person whom the Merchant authorizes to use Merchant Device and/or Merchant Portal.

1.7. **Luminor Phone POS service** – a service provided by the Bank for acceptance of payment cards by means of the - Luminor Phone POS installed on Merchant Device.

1.8. **Luminor Phone POS** – an application available on Google Play.

1.9. **Rules** – Card Acceptance Rules the annex of which are these Special Provisions.

1.10. **Password** – a password set up by the Merchant within the Luminor Phone POS app that enables access to the Luminor Phone POS.

2. To use Luminor Phone POS Service, the merchant receives an email message containing a unique link to access the password setup module, sets his personal password; downloads the application (if not yet done before this step); opens up the downloaded Luminor Phone POS application, enters his Merchant Credentials and accepts all the required permissions to be enabled for the application to work.

3. The Merchant's Device must have a stable internet connection and NFC technology available and activated to utilize Luminor Phone POS service.

4. The Merchant indicates the email for each device that the Merchant intends to use as the Merchant's Device in the Application for the use of Luminor Phone POS service and/or the Agreement. The Merchant may change this information (add/remove device) by sending a written notice acceptable to the Bank by form and content to the Bank. The Bank performs an evaluation of the proposed changes within 3 (three) Business Days. If the change is acceptable to the Bank, the Merchant`s written notice is considered to be part of the Agreement and the Bank performs the required actions to

ierosināto izmaiņu ieviešanai. Banka ir tiesīga atteikties pieņemt ierosinātās izmaiņas, informējot par to Komersantu.

5. Komersants sedz izmaksas, kas saistītas ar Luminor Phone POS pakalpojuma ieviešanu un izmantošanu, kā arī nodrošina savietojamu ierīci un interneta pieslēgumu.

6. Pirmā parole tiek iestatīta, izmantojot Luminor sniegto saiti. Komersantam jāiestata Parole Luminor Phone POS katrā Komersanta ierīcē. Komersants ir atbildīgs par Paroles maiņu pēc Bankas pieprasījuma un gadījumos, kad Komersantam ir aizdomas par Luminor Phone POS pakalpojuma nesankcionētu vai krāpniecisku izmantošanu.

7. Komersantam ir jāglabā Komersanta akreditācijas dati noslēpumā un tie nevienam nav jāatklāj. Komersantam ir arī jānodrošina, ka katrā Komersanta ierīcē ir iestatīta ekrāna bloķēšana un neviena nesankcionēta persona nevar piekļūt nevienai Komersanta ierīcei. Ja Komersants neievēro kādu no šiem pienākumiem, Banka nav atbildīga par jebkādiem zaudējumiem un/vai bojājumiem, kas radušies Komersantam un/vai jebkurai trešai personai, un Komersants apņemas atlīdzināt visus Bankai un/vai jebkurai citai trešai personai radušos zaudējumus.

8. Komersantam nekavējoties jāinformē Banka, ja Komersantam ir pamats aizdomām par nesankcionētu piekļuvi Komersanta akreditācijas datiem vai Komersanta ierīcei. Kamēr Banka nav saņēmusi un apliecinājusi šādu paziņojumu, tā nav atbildīga par jebkādiem zaudējumiem un/vai bojājumiem, kas radušies Komersantam un/vai trešai personai sakarā ar nesankcionētu piekļuvi Komersanta akreditācijas datiem vai Komersanta ierīcei, un Komersantam jāatlīdzina visus Bankai un/vai jebkurai citai trešai personai radušos zaudējumus.

9. Komersantam ir jāievēro Bankas un/vai Luminor Phone POS izstrādātāja sniegtā lietotāja rokasgrāmata un norādījumi par Luminor Phone POS lietotnes izmantošanu.

10. Izmantojot Luminor Phone POS pakalpojumu, ir pieejami tikai Darījumi tikai EUR valūtā, kas veikti ar Visa vai Mastercard maksājumu kartēm.

11. Komersantam pēc pieprasījuma jāiesniedz Kartes lietotājam darījuma kvīts, izmantojot Luminor Phone POS pieejamos līdzekļus pa e-pastu vai skenējot QR kodu.

effect the proposed change. The Bank is entitled to refuse to accept the proposed changes, by informing the Merchant thereof.

5. The Merchant bears the costs related to the implementation and use of the Luminor Phone POS service, including ensuring a compatible device and internet connection.

6. The first password is set via the link provided by Luminor. The Merchant must set a Password within the Luminor Phone POS on each Merchant's Device. The Merchant is responsible for changing of the Password upon Bank's request and in cases when the Merchant suspects unauthorized or fraudulent use of Luminor Phone POS service.

7. The Merchant must keep its Credentials secret and not disclose them to anyone. The Merchant must also ensure that a screen lock is set up on each Merchant's Device and no unauthorized person can access any Merchant's Device. If the Merchant fails to observe any of these obligations, the Bank is not liable for any loss and/or damages incurred by the Merchant and/or any third party and the Merchant shall undertake to reimburse any loss suffered by the Bank and/or any third party.

8. The Merchant must notify the Bank immediately if the Merchant has reasons to suspect unauthorized access to the Merchant's Credentials or the Merchant's Device. Until the Bank has received and acknowledged such notification, the Bank is not liable for any loss and/or damages incurred by the Merchant and/or third party due to unauthorized access to the Merchant's Credentials or the Merchant's Device and the Merchant shall be responsible to reimburse any loss suffered by the Bank and/or any third party.

9. The Merchant must follow the user manual and instructions on use of the Luminor Phone POS, prepared by the Bank and developer of the Luminor Phone POS.

10. Only EUR Transactions performed using Visa or Mastercard payment cards are available using the Luminor Phone POS service.

11. The Merchant must provide the Card User with the transaction receipt upon request by means available within the Luminor Phone POS via email or scanning QR code.

KOMERSANTA PORTĀLS

12. Banka var ļaut Komersantam piekļuvi Komersanta portālam atbilstoši Bankas ieskatiem.

13. Komersanta portāla funkcionalitāte (tostarp Pakalpojumu veids un tvērums, kas Lietotājam ir pieejami Komersanta portālā) un pieejamība (tostarp Pakalpojumu sniegšanas laiks un ierobežojumi Komersanta portālā) tiek noteikta Komersanta portāla vidē, attiecīgā Pakalpojuma pakalpojumu noteikumos un/vai Bankas tīmekļa vietnē. Lietotājam jāievēro Bankas norādījumi, izmantojot Komersanta portālu un pieejamos Pakalpojumus.

14. Komersants norāda Administratoru Līgumā un/vai Pieteikumā, un/vai citos Bankas noteiktos veidos. Dokuments, kur Komersants norāda Administratoru, tiek uzskatīts par pilnvarojumu. Komersants var atcelt un/vai mainīt Administratoru šeit aprakstītajā veidā.

15. Administrators Komersanta vārdā var pievienot un dzēst Lietotājus, apturēt un atjaunot apturētās lietošanas tiesības, kas piešķirtas Lietotājam, kā arī iestatīt un mainīt Komersanta portāla lietošanas režīmu, kas piešķirts Lietotājam Komersanta portālā (ja tehniski iespējams) vai citos Bankas noteiktos veidos. Banka ir tiesīga pieprasīt, lai jebkāds no iepriekš minētajiem pieprasījumiem tiek iesniegts rakstiski un/vai parakstīts Bankas pārstāvja klātbūtnē.

16. Lietotāja tiesību tvērums piekļūt Pakalpojumiem, izmantojot Komersanta portālu, tiek noteikts ar Komersanta portāla lietošanas režīmu, kas norādīts Komersanta portāla vidē vai jebkur citur, kā to nosaka Banka.

17. Banka aktivizēs, apturēs, atjaunos un izbeigs Lietotāja spēju izmantot Komersanta portālu saprātīgā laikā pēc tam, ir izpildīti Īpašajos noteikumos paredzētie nosacījumi. Lietotāja tiesības saņemt Pakalpojumus, izmantojot Komersanta portālu, kā arī to izmaiņas stājas spēkā, kad tās ir reģistrētas attiecīgajā Bankas informācijas sistēmā.

18. Banka autentificē Lietotāju, kurš vēlas izmantot Komersanta portālu, pēc tās ieskatiem ar vienu vai vairākiem Autentifikācijas līdzekļiem.

19. Lai izmantotu Autentifikācijas līdzekli, Lietotājam varētu būt nepieciešams instalēt konkrētu programmatūru un/vai izmantot konkrētu aprīkojumu. Banka var noteikt prasības šādai programmatūrai un aprīkojumam, kā arī mainīt šādas prasības jebkurā laikā, tostarp definēt, ka

MERCHANT PORTAL

12. The Bank may enable the Merchant access to Merchant Portal upon Bank's sole discretion.

13. The functionality (including the type and scope of Services, which are available to the User via the Merchant Portal) and availability (including the time and restrictions of provision of the Services via the Merchant Portal) of the Merchant Portal is determined in the environment of the Merchant Portal, in the Service Terms of the respective Service and/or on the Bank's website. The User must observe the Bank's instructions in using the Merchant Portal and the Services available.

14. The Merchant indicates Administrator in the Agreement and/or the Application and/or by other means set by the Bank. Document where the Merchant indicates Administrator is considered to be an authorization document. The Merchant may revoke and/or change Administrator in the manner described herein.

15. The Administrator may, on behalf of the Merchant, add and remove Users, suspend and restore suspended usage rights assigned to a User as well as set and change the mode of use of the Merchant Portal assigned to a User within the Merchant Portal (if technically possible) or by other means defined by the Bank. The Bank is entitled to request that any of the requests above are submitted in writing and/or signed in the presence of a representative of the Bank.

16. The scope of the User's rights to access the Services using the Merchant Portal is determined by the mode of use of the Merchant Portal indicated within the Merchant Portal environment or elsewhere as set by the Bank.

17. The Bank will activate, suspend, restore and terminate the User's ability to use the Merchant Portal within a reasonable time after the conditions envisaged in the Special Provisions are fulfilled. The User's rights to receive the Services using the Merchant Portal, as well as changes thereto enter into force, when those are registered in the respective Bank's information system.

18. The Bank authenticates the User, who wants to use the Merchant Portal, at its discretion by one or more Authentication Instruments.

19. To use an Authentication Instrument, the User may need to install certain software and/or use certain equipment. The Bank can set requirements for such

Autentifikācijas līdzekļa lietošanai ir nepieciešama konkrēta programmatūra un/vai aprīkojums. Lietotājam jānodrošina šo prasību izpilde par saviem līdzekļiem.

20. Banka var definēt, ka konkrētie Autentifikācijas līdzekļi, programmatūra un/vai aprīkojums jāizmanto, lai saņemtu konkrētus Pakalpojumus un/vai atļautu konkrētus Darījumus (tostarp atmaksas). Banka arī var noteikt, ka, izmantojot konkrētus Autentifikācijas līdzekļus, konkrēti Pakalpojumi ir pieejami un/vai pieejamo Pakalpojumu funkcionalitāte ir ierobežota un/vai atšķiras.

21. Ja Autentifikācijas līdzekli, aprīkojumu un/vai programmatūru, kas rada, reģistrē, apstiprina un/vai veic citas darbības saistībā ar Autentifikācijas līdzekli, izsniedz Banka, Lietotājs var to saņemt pēc tam, kad ir izpildīti attiecīgajos Pakalpojumu noteikumos paredzētie nosacījumi. Komersantam jāmaksā Bankai Cenrādī norādītā maksa par šāda līdzekļa, aprīkojuma un/vai programmatūras nodrošināšanu, ja vien Puses nevienojas citādi.

22. Ja Autentifikācijas līdzekli, aprīkojumu un/vai programmatūru, kas rada, reģistrē, apstiprina un/vai veic citas darbības saistībā ar Autentifikācijas līdzekli, izsniedz trešā persona, Banka nav atbildīga par to darbību un drošību, kā arī par jebkuriem zaudējumiem, kas radušies Lietotājam, Komersantam un/vai trešai personai saistībā ar šāda Autentifikācijas līdzekļa, aprīkojuma un/vai programmatūras lietošanu.

23. Ja Lietotājs ir norādījis Autentifikācijas līdzeklī izmantotos datus, Lietotājs var tos mainīt, iesniedzot Bankai paziņojumu Bankas noteiktajā kārtībā.

24. Ja saskaņā ar Autentifikācijas līdzekļa lietošanas nosacījumiem ir paredzēts, ka kaut kas var tikt nosūtīts uz Lietotāja aprīkojumu (piemēram, SMS koda nosūtīšana uz mobilo tālruni), tad Lietotājs ir atbildīgs par Bankai sniegtā identifikatora pareizību, kas tiek izmantots šādas informācijas nosūtīšanai (piemēram, tālruņa numurs). Ja Lietotājs maina aprīkojumu un/vai tā identifikatoru, Lietotājam par to nekavējoties jāpaziņo Bankai. Līdz šāda paziņojuma saņemšanai Banka turpina attiecīgā Autentifikācijas līdzekļa nosūtīšanu, izmantojot Bankai pieejamo identifikatoru. Šādā gadījumā Banka nav atbildīga par zaudējumiem, kas radušies Komersantam, Lietotājam un/vai trešām personām.

25. Banka var pieprasīt un šajā gadījumā Lietotājam ir jāaizstāj Autentifikācijas līdzeklis pret citu Bankas norādītu Autentifikācijas līdzekli un/vai jāmaina Autentifikācijas līdzeklī izmantotie dati.

software and equipment, as well as change such requirements at any time, including to define that the use of an Authentication Instrument requires specific software and/or equipment. The User must ensure the fulfillment of these requirements at their expense.

20. The Bank can define that certain Authentication Instruments, software and/or equipment must be used for reception of particular Services and/or authorisation of particular Transactions (including refunds). The Bank can also set that by using certain Authentication Instrument certain Services are available and/or the functionality of available Services is limited and/or differ.

21. If the Authentication Instrument, equipment and/or software, which creates, registers, validates and/or performs other actions in relation to an Authentication Instrument, is issued by the Bank, the User may receive it after the conditions prescribed in the respective Service Terms are met. The Merchant must pay to the Bank the fee indicated in the Price List for provision of such an instrument, equipment and/or software, unless the Parties agree otherwise.

22. If the Authentication Instrument, equipment and/or software, which creates, registers, validates and/or performs other actions in relation to an Authentication Instrument, is issued by a third party, the Bank is not liable for their operation and security, as well as for any damages incurred by the User, the Merchant and/or a third party in relation to the use of such an Authentication Instrument, equipment and/or software.

23. If the data used in the Authentication Instrument are indicated by the User, the User may change them by submitting a notice to the Bank according to the procedure set by the Bank.

24. If according to the conditions of the use of the Authentication Instrument, it is envisaged that something may be sent to the User's equipment (for example, sending an SMS code to a mobile phone), then the User is responsible for the correctness of the identifier provided to the Bank, which is used for sending of such information (for example, a phone number). If the User changes the equipment and/or its identifier, the User must notify the Bank thereof immediately. Until such a notice is received, the Bank continues sending the respective Authentication Instrument, using the identifier available to the Bank. In such a case, the Bank is not liable for any damages incurred by the Merchant, the User and/or third parties.

26. Lietotājam, kurš izmanto Autentifikācijas līdzekli, ir jāievēro attiecīgā Autentifikācijas līdzekļa lietošanas nosacījumi, kā arī tā izsniedzēja norādījumi, tostarp jānodrošina saderīgs aprīkojums un/vai programmatūra veiksmīgai Autentifikācijas līdzekļa lietošanai, kā arī jāievēro šāda aprīkojuma un/vai programmatūras ražotāja un/vai izsniedzēja noteikumi un/vai norādījumi.

27. Banka var atteikties sniegt Pakalpojumu, izmantojot Komersanta portālu, ja Lietotājs neizpilda šo Īpašo noteikumu nosacījumus.

28. Ja Autentifikācijas līdzeklis ir veiksmīgi izmantots, lai apstiprinātu kādu darbību (piemēram, piekļūtu Komersanta portālam, atļautu atmaksu, pievienotu/noņemtu Lietotāju, bloķētu/atbloķētu Komersanta ierīci utt.), tiek uzskatīts, ka Lietotājs, kuram atbilst (pieder, ir reģistrēts, ir izsniegts, ir rīcībā utt.) attiecīgais Autentifikācijas līdzeklis, ir apstiprinājis šādu darbību klātienē (ieskaitot, ka elektroniskais dokuments, kas parakstīts ar Autentifikācijas līdzekli, uzskatāms par parakstītu ar roku). Šāds dokuments ir saistošs Komersantam, Lietotājam un Bankai.

29. Visa informācija, ko Banka sniedz, izmantojot Komersanta portālu, ir saistoša Lietotājam un Komersantam un ir līdzvērtīga Bankas parakstītam dokumentam.

30. Ja Lietotājs izmanto Autentifikācijas līdzekļus, lai piekļūtu vai saņemtu trešo personu pakalpojumus, Banka nav atbildīga par šiem pakalpojumiem, kā arī neatlīdzina zaudējumus, kas Lietotājam, Komersantam un/vai trešai personai radušies saistībā ar šādu pakalpojumu izmantošanu vai šādu trešo personu darbību vai bezdarbību.

31. Banka var ierakstīt un reģistrēt darbības, kas veiktas, izmantojot Komersanta portālu, un uzglabāt šo informāciju Bankas un/vai trešo personu datubāzēs. Šie ieraksti ir pierādījums un apliecinājums Komersanta gribai un var kalpot kā pierādījums strīdu izšķiršanai starp Pusēm, tostarp tiesā. Banka var, bet tai nav pienākums, glabāt ierakstus līdz 10 (desmit) gadiem pēc Pušu darījuma attiecību izbeigšanās.

25. The Bank may request and in this case the User must replace the Authentication Instrument with another Authentication Instrument indicated by the Bank and/or change the data used in the Authentication Instrument.

26. The User who uses an Authentication Instrument, must observe usage conditions of the respective Authentication Instrument, as well as issuer's instructions, including to ensure compatible equipment and/or software for successful use of the Authentication Instrument, as well as to observe rules and/or instructions of the manufacturer and/or issuer of such equipment and/or software.

27. The Bank can refuse to provide a Service using the Merchant Portal, if the User does not fulfill conditions of these Special Provisions.

28. If an Authentication Instrument has been successfully used to approve any action (e.g., access the Merchant Portal, authorize a refund, add/remove User, block/unblock Merchant Device etc.), it is considered that the User, to whom the respective Authentication Instrument corresponds (belongs to, is registered to, has been issued to, is at disposal etc.), has approved such action in person (including that the electronic document which is signed using an Authentication Instrument shall be considered to have been signed by handwritten signature). Such a document is binding on the Merchant, the User and the Bank.

29. All information provided by the Bank using the Merchant Portal, is binding on the User and the Merchant and is equivalent to a document signed by the Bank.

30. If the User uses Authentication Instruments to access or receive third-party services, the Bank is not responsible for such services, nor shall compensate damages, which the User, the Merchant and/or a third party incurred in relation to the use of such services or activity or inactivity of such third parties.

31. The Bank may record and register actions performed using the Merchant Portal and store this information in databases of the Bank and/or third parties. These records are evidence and certification of the Merchant's will and may serve as evidence for resolution of disputes between the Parties, including in a court. The Bank can, but is not obligated to store the records for up to 10 (ten) years after termination of the business relationship between the Parties.