Specialiosios „Luminor Phone POS“ mokėjimo kortelių aptarnavimo nuostatos

1 Priedas prie Mokėjimo kortelių aptarnavimo taisyklių

Kartu su kitomis Taisyklių nuostatomis, šios Specialiosios „Luminor Phone POS“ mokėjimo kortelių aptarnavimo nuostatos (toliau – **Specialiosios nuostatos**) yra taikomos Sutarties šalių tarpusavio santykiams, susijusiems su „Luminor Phone POS“ paslaugos, kaip ji apibrėžta šiame 1 priede, teikimu. Jeigu šio 1 priedo nuostatos prieštarauja kitoms Taisyklių nuostatoms, pirmenybė yra teikiama 1 priedo nuostatoms tiek, kiek jos taikytinos „Luminor Phone POS“ paslaugai.

1. Toliau šiose Specialiosiose nuostatose vartojamos sąvokos turi tokią reikšmę

   1.1. **Administratorius** – Naudotojas, kuriam Prekybininkas suteikė įgaliojimus administruoti Naudotojų naudojimosi Prekybininko portalu teises.

   1.2. **Autentiškumo patvirtinimo priemonės** – elementai, kurie pagal Banko nustatytas procedūras leidžia patvirtinti asmens autentiškumą ir (arba) patikrinti konkrečios mokėjimo priemonės naudojimo pagrįstumą, įskaitant personalizuotus autentifikavimo duomenis, pavyzdžiui, naudotojo (kliento) numerį, prisijungimo vardą, kodą, slaptažodį, telefono numerį, įrenginio duomenis (pavyzdžiui, serijos numerį, IMEI numerį), asmens duomenis (pavyzdžiui, vardą, pavardę, asmens kodą), įskaitant biometrinius duomenis (pavyzdžiui, pirštų atspaudus, skaitmeninį veido atvaizdą, akies rainelės atvaizdą, balso įrašą ir kt.), taip pat elektroninis parašas (elektroninius duomenis gali sudaryti bet kuris iš pirmiau minėtų elementų ir (arba) kiti elektroniniai duomenys), kvalifikuotas elektroninis parašas ir kt.

   1.3. „**Luminor Phone POS**“ – programėlė, kurią

Special Provisions for Luminor Phone POS Card Acceptance

Annex 1 for Payment 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 to the Agreement 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. **Luminor Phone POS** – an application available on Google Play

   1.4. **Luminor Phone POS services** – a mobile application for the acceptance of Cards by means of the Luminor Phone POS app installed

galima įsidiegti per „Google Play“.

1.4. „**Luminor Phone POS**“ paslaugos – mobilioji aplikacija, kuri skirta Kortelėms aptarnauti naudojantis programėle „Luminor Phone POS“, įdiegta Prekybininko įrenginyje.

1.5. **Naudotojas** – fizinis asmuo, kuriam Prekybininkas suteikė įgaliojimus naudotis Prekybininko įrenginiu ir (arba) Prekybininko portalu.

1.6. **Prekybininkas** – šių Specialiųjų nuostatų tikslais suprantamas kaip Klientas, apibrėžtas Taisyklių 1.13 punkte.

1.7. Prekybininko įrenginys – bet kuris įrenginys, naudojantis programėlę bet kuriame įrenginyje, kuriame veikia „Android 9“ ar vėlesnė šios mobiliosios operacinės sistemos versija ir artimojo lauko ryšio (NFC) funkcija, taip pat kuris iš pradžių buvo pristatytas (įgytas) su „Android 8“ ar vėlesnė versija bei kuris yra užregistruotas naudojimuisi „Luminor Phone POS“ paslauga, naudojant Prekybininko prisijungimo duomenis.

1.8. **Prekybininko portalas** – skaitmeninis kanalas, leidžiantis Prekybininkui atlikti atitinkamus su „Luminor Phone POS“ paslauga susijusius veiksmus.

1.9. **Prekybininko prisijugimo duomenys** – informacija, kuri skirta susikurti prisijungimo prie „Luminor Phone POS“ slaptažodį, gaunama el. paštu, nurodytu Prašyme.

1.10. **Slaptažodis** – „Luminor Phone POS“ programėlėje Prekybininko susikurtas slaptažodis, kuris leidžia prisijungti prie „Luminor Phone POS“ programėlės.

1.11. **Taisyklės** – Mokėjimo kortelių aptarnavimo taisyklės, kurių priedas yra šios Specialiosios nuostatos.

2. Tam, kad galėtų naudotis „Luminor Phone POS“ paslauga, Prekybininkas gauna el. laišką su unikalia nuoroda į slaptažodžio nustatymo modulį, kur susikuria savo asmeninį slaptažodį; įsidiegia programėlę (jei to dar nepadarė iki šio žingsnio); atidaro atsisiųstą ir įsidegtą „Luminor Phone POS“ programėlę, suveda Prekybininko prisijungimo duomenis ir sutinka su visais reikiamais leidimais, kad programėlė veiktų.

3. Prekybininko įrenginyje turi būti stabilus interneto

on Merchant Device.

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

1.6. **Merchant** – for the purposes of these Special Provisions is considered as Client defined under section 1.13 of the Rules.

1.7. **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.

1.8. **Merchant Portal** – a Digital channel enabling the Merchant to perform specific activities related to Luminor Phone POS Service.

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

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

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

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 an application 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

ryšys bei veikianti ir aktyvuota NFC technologija tam, kad būtų galima naudotis „Luminor Phone POS“ paslauga.

4. Prašyme leisti naudotis „Luminor Phone POS“ paslauga ir (arba) pačioje Sutartyje Prekybininkas nurodo po el. pašto adresą kiekvienam įrenginiui, kurį ketina naudoti kaip Prekybininko įrenginį. Šią informaciją Prekybininkas gali pakeisti (pridėti / pašalinti įrenginį), išsiųsdamas Bankui priimtinos formos ir turinio prašymą. Bankas per 3 (tris) darbo dienas atlieka šių siūlomų pakeitimų įvertinimą. Jei siūlomas pakeitimas Bankui yra priimtinas, rašytinis pranešimas tampa Sutarties dalimi ir Bankas atlieka reikiamus veiksmus tam, kad būtų atliktas šis pakeitimas. Bankas turi teisę atsisakyti sutikti su siūlomais pakeitimais, atitinkamai informuodamas Prekybininką.

5. Prekybininkui tenka su „Luminor Phone POS“ paslaugos diegimu ir naudojimusi susijusios išlaidos, įskaitant išlaidas dėl suderinamo įrenginio bei interneto ryšio užtikrinimo.

6. Pirmasis Slaptažodis yra susikuriamas per „Luminor“ suteiktą nuorodą. Prekybininkas turi susikurti Slaptažodį „Luminor Phone POS“ programėlei naudoti kiekviename Prekybininko įrenginyje. Prekybininkas privalo pakeisti Slaptažodį Bankui to paprašius arba kai pats Prekybininkas įtaria, kad „Luminor Phone POS“ paslauga galimai naudojamasi neautorizuotai ir nesąžiningai.

7. Prekybininkas turi pareigą saugoti ir niekam neatskleisti savo prisijungimo duomenų. Prekybininkas taip pat turi pareigą užtikrinti, kad kiekviename Prekybininko įrenginyje būtų nustatytas ekrano užraktas ir joks asmuo be leidimo negalėtų prisijungti prie nė vieno iš Prekybininko įrenginių. Prekybininkui nesilaikant šių įsipareigojimų, Bankas neatsako už bet kokius Prekybininko ir (arba) trečiosios šalies patirtus nuostolius ir (arba) žalą, o Prekybininkas įsipareigoja atlyginti bet kokius Banko ir (arba) trečiosios šalies patirtus nuostolius.

8. Jeigu Prekybininkas turi pagrindo įtarti, kad prie Prekybininko įrenginio buvo neteisėtai prisijungta arba neteisėtai nusavinti Prekybininko prisijungimo duomenys, Prekybininkas privalo nedelsiant apie tai pranešti Bankui. Kol Bankas nėra gavęs ir patvirtinęs tokio pranešimo, Bankas neatsako už bet kokius nuostolius ir (arba) žalą, kurią Prekybininkas ir (arba) trečioji šalis patyrė dėl neautorizuotos prieigos prie Prekybininko prisijungimo duomenų ar Prekybininko įrenginio, o Prekybininkas privalo atlyginti bet kokius Banko ir (arba) trečiosios šalies patirtus nuostolius.

acceptable to the Bank, the written notice is considered to be part of the Agreement and the Bank performs the required actions to 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 made available by the Bank an/or the developer of the Luminor Phone POS as well as instructions of the Bank and developer of the Luminor Phone POS for the use 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 user of the Card (Cardholder) with the transaction receipt upon request by means available within the Luminor Phone POS service via email or scanning QR code.

9. Prekybininkas privalo vadovautis Banko ir (arba) „Luminor Phone POS“ programėlės kūrėjo pateiktu naudotojo vadovu, taip pat Banko ir (arba) „Luminor Phone POS“ programėlės kūrėjo instrukcijomis dėl „Luminor Phone POS“ programėlės naudojimo.

10. Naudojantis „Luminor Phone POS“ paslauga yra galimos tik Operacijos eurais ir tik naudojantis „Visa“ arba „Mastercard“ Kortelėmis.

11. Prekybininkas privalo pateikti Kortelės turėtojui, kai šis prašo, Operaciją patvirtinantį Kvitą naudodamasis „Luminor Phone POS“ paslaugoje prieinamomis priemonėmis – el. paštu arba leisdamas nuskaityti QR kodą.

PREKYBININKO PORTALAS

12. Bankas turi teisę išimtinai savo nuožiūra spręsti dėl prieigos prie Prekybininko portalo Prekybininkui suteikimo.

13. Prekybininko portalo funkcionalumas (įskaitant paslaugų, kuriomis Naudotojas gali naudotis per Prekybininko portalą, rūšį ir apimtį) ir prieinamumas (įskaitant paslaugų teikimo per Prekybininko portalą laiką ir apribojimus) yra nustatomas Prekybininko portalo aplinkoje atitinkamos paslaugos teikimo sąlygose ir (arba) Banko interneto svetainėje. Naudotojas, naudodamasis Prekybininko portalu, taip pat ir prieinamomis paslaugomis, privalo laikytis Banko nurodymų.

14. Prekybininkas Sutartyje ir (arba) Prašyme ir (arba) kitokiais Banko nustatytais būdais nurodo Administratorių. Atitinkamai dokumentas, kuriame Prekybininkas nurodo Administratorių, yra laikomas autorizuojančiu dokumentu. Prekybininkas tokiu pačiu būdu gali atšaukti ir (arba) pakeisti Administratorių kaip šiame punkte nustatyta.

15. Administratorius, Prekybininko vardu, gali pridėti ir pašalinti Naudotojus, sustabdyti ir atstatyti jau sustabdytas Naudotojui priskirtas naudojimosi teises, taip pat nustatyti ir keisti Naudotojui priskirtą naudojimosi Prekybininko portalu režimą Prekybininko portale (jei tai techniškai įmanoma) arba kitais Banko nustatytais būdais. Bankas turi teisę reikalauti, kad bet kuris iš pirmiau nurodytų prašymų būtų pateiktas raštu ir (arba) pasirašytas dalyvaujant Banko atstovui.

16. Naudotojo teisių naudotis paslaugomis per Prekybininko portalą apimtis yra nustatoma pagal Prekybininko portalo naudojimo būdą, nurodytą Prekybininko portalo aplinkoje arba kita Banko nustatyta tvarka.

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

17. Bankas aktyvuos, sustabdys, atstatys ir nutrauks Naudotojo galimybę naudotis Prekybininko portalu per protingą laiką po to, kai bus įvykdytos Specialiosiose nuostatose numatytos sąlygos. Naudotojo teisė gauti paslaugas per Prekybininko portalą, taip pat jų pakeitimai įsigalioja, kai jie užregistruojami atitinkamoje Banko informacinėje sistemoje.

18. Naudotojo, norinčio naudotis Prekybininko portalu, autentiškumą Bankas patvirtina savo nuožiūra viena arba keliomis Autentiškumo patvirtinimo priemonėmis.

19. Kad galėtų naudotis Autentiškumo patvirtinimo priemone, Naudotojui gali reikėti naudoti tam tikrą įrangą ir (arba) įsidiegti tam tikrą programinę įrangą. Bankas gali nustatyti reikalavimus tokiai įrangai bei programinei įrangai, taip pat bet kuriuo metu pakeisti šiuos reikalavimus, taip pat nustatyti, kad Autentiškumo patvirtinimo priemonės naudojimui bus reikalinga konkreti arba speciali įranga ir (arba) programinė įranga. Naudotojas privalo savo sąskaita užtikrinti tokių reikalavimų įvykdymą.

20. Bankas be kita ko gali nustatyti, kad tam tikros Autentiškumo patvirtinimo priemonės, programinė įranga ir (arba) įranga privalo būti naudojami tam tikroms paslaugoms gauti ir (arba) tam tikroms Operacijoms (įskaitant pinigų grąžinimą) vykdyti. Bankas taip pat gali nustatyti ir tai, kad naudojant tam tikrą Autentiškumo patvirtinimo priemonę galima gauti tam tikras paslaugas ir (arba) kad būtų ribojamas ir (arba) skirtingas teikiamų paslaugų funkcionalumas.

21. Jeigu Autentiškumo patvirtinimo priemonę, įrangą ir (arba) programinę įrangą, kuri sukuria, užregistruoja, patvirtina ir (arba) atlieka kitus veiksmus, susijusius su Autentiškumo patvirtinimo priemone, išduoda Bankas, Naudotojas gali ją gauti, kai įvykdomi atitinkamose paslaugų teikimo sąlygose nustatyti reikalavimai. Už tokios priemonės, įrangos ir (arba) programinės įrangos suteikimą Prekybininkas moka Bankui Kainyne nurodytą mokestį, išskyrus atvejus, kai šalys sutaria kitaip.

22. Jeigu Autentiškumo patvirtinimo priemonė, įranga ir (arba) programinė įranga, kuri sukuria, užregistruoja, patvirtina ir (arba) atlieka kitus veiksmus, susijusius su Autentiškumo patvirtinimo priemone, yra išduota trečiosios šalies, Bankas neatsako už jų veikimą bei saugumą, taip pat ir už bet kokią Naudotojo, Prekybininko ir (arba) trečiosios šalies žalą, kuri būtų patirta dėl tokios Autentiškumo patvirtinimo priemonės, įrangos ir (arba) programinės įrangos naudojimo.

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 authorization 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.

23. Jeigu Autentiškumo patvirtinimo priemonėje naudojamus duomenis nurodė Naudotojas, jis taip pat gali juos ir pakeisti pateikdamas Bankui pranešimą Banko nustatyta tvarka.

24. Jeigu pagal Autentiškumo patvirtinimo priemonės naudojimo sąlygas nustatyta, kad į Naudotojo įrangą gali būti kas nors siunčiama (pavyzdžiui, yra siunčiamas SMS kodas į mobilųjį telefoną), Naudotojas visiškai atsako už Bankui pateikto identifikatoriaus, kuris naudojamas tokiai informacijai siųsti (pavyzdžiui, telefono numerio), teisingumą. Jei Naudotojas pakeičia įrangą ir (arba) jos identifikatorių, jis privalo nedelsdamas apie tai pranešti Bankui. Kol toks pranešimas negautas, Bankas toliau siunčia atitinkamą Autentiškumo patvirtinimo priemonę naudodamasis tuo identifikatoriumi, kuris Bankui yra prieinamas. Tokiu atveju Bankas neatsako už jokių Prekybininko, Naudotojo ir (arba) trečiųjų šalių patirtą žalą.

25. Bankas gali pareikalauti ir tokiu atveju Naudotojas privalo pakeisti Autentiškumo patvirtinimo priemonę kita Banko nurodyta Autentiškumo patvirtinimo priemone ir (arba) pakeisti Autentiškumo patvirtinimo priemonėje naudojamus duomenis.

26. Naudotojas, kuris naudoja Autentiškumo patvirtinimo priemonę, privalo laikytis atitinkamos Autentiškumo patvirtinimo priemonės naudojimo sąlygų, taip pat jos išdavėjo nurodymų, įskaitant užtikrinti suderinamą įrangą ir (arba) programinę įrangą sėkmingam Autentiškumo patvirtinimo priemonės naudojimui, taip pat laikytis tokios įrangos ir (arba) programinės įrangos gamintojo ir (arba) išdavėjo taisyklių ir (arba) nurodymų.

27. Bankas gali atsisakyti teikti Naudotojui paslaugą naudojantis Prekybininko portalu, jei Naudotojas nevykdo šių Specialiųjų nuostatų sąlygų.

28. Jeigu Autentiškumo patvirtinimo priemonė buvo sėkmingai panaudota bet kokiam veiksmui patvirtinti (pvz., prisijungti prie Prekybininko portalo, autorizuoti pinigų grąžinimą, pridėti ir (arba) pašalinti Naudotoją, užblokuoti ir (arba) atblokuoti Prekybininko įrenginį ir t. t.), laikoma, kad Naudotojas, kuriam atitinkama Autentiškumo patvirtinimo priemonė yra priskirta (jam priklauso, jo vardu užregistruota, jam buvo išduota, yra jo žinioje ir t. t.), asmeniškai patvirtino tokį veiksmą (įskaitant tai, kad elektroninis dokumentas, kuris pasirašytas naudojant Autentiškumo patvirtinimo priemonę, yra prilyginamas ranka pasirašytam dokumentui). Toks dokumentas yra privalomas vykdyti Prekybininkui, Naudotojui ir Bankui.

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 to the Agreement, including 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.

29. Visa Banko pateikia informacija jam naudojantis Prekybininko portalu saisto Naudotoją ir Prekybininką ir yra prilyginama Banko pasirašytam dokumentui.

30. Jei Naudotojas naudoja Autentiškumo patvirtinimo priemones trečiųjų šalių paslaugoms pasiekti ar gauti, Bankas neatsako už tokias paslaugas ir neatlygina žalos, kurią Naudotojas, Prekybininkas ir (arba) trečioji šalis patyrė dėl naudojimosi tokiomis paslaugomis arba dėl tokių trečiųjų šalių veiklos ar neveikimo.

31. Bankas gali fiksuoti (saugoti) ir registruoti veiksmus, atliktus naudojantis Prekybininko portalu, ir saugoti šią informaciją Banko ir (arba) trečiųjų šalių duomenų bazėse. Šie įrašai yra Prekybininko išreikštos valios įrodymas ir patvirtinimas ir gali būti naudojami kaip įrodymai sprendžiant tarp Sutarties šalių kilusius ginčus, taip pat ir ginčus teisme. Bankas gali, tačiau neprivalo saugoti įrašus iki 10 (dešimties) metų po Sutarties šalių verslo santykių nutraukimo.