Bank Pocztowy S.A.

Electronic and Telephone Banking

Terms and Conditions

2021

Table of Contents

Part I. General

Clause 1

These Terms and Conditions shall govern the provision by the Bank of the Electronic and Telephone Banking Services to Service Users in connection with their use of Bank products or services.

Clause 2

1. As used in these Terms and Conditions, the following terms shall have the respective meanings as defined below:
   1) **BLIK Nickname (or Alias)** shall mean an individual User Service identifier used when making certain BLIK Mobile Payments;
   2) **Mobile Application** shall mean an application made available by the Bank as part of the Electronic Banking Service, installed by the Service User on a mobile device, and enabling delivery and use of Bank products and services under the Product Agreement;
   3) **Authorisation** shall mean the Service User's consent to executing an Instruction, expressed as required under the Product Agreement via the Electronic Banking Service or Telephone Banking Service;
   4) **Bank** shall mean Bank Pocztowy Spółka Akcyjna, with its registered office at ul. Jagiellońska 17, 85-959 Bydgoszcz, Poland, entered in the business register maintained by the District Court of Bydgoszcz, 13th Commercial Division of the National Court Register, under No. KRS 0000010821, with a share capital of PLN 128,278,080 (paid up in full), Tax Identification Number (NIP) 5540314271, which is a Payment Service Provider as defined in the Payment Services Act;
   5) **Cashback** shall mean a service whereby cash can be withdrawn at a point of sale in Poland when performing a cashless debit card transaction or BLIK Mobile Payment;
   6) **Contact Centre** shall mean the Bank's customer care services, including the Bank Helpline, live chat and dedicated email address, as specified on the Bank Website;
   7) **Biometric Data** shall mean sensitive personal data as defined in Article 4(14) of the GDPR, which also include the Service User's behavioural characteristics;
   8) **Instruction** shall mean an order placed by the Service User with the Bank, including a Payment Order or another declaration of intent or assertion of fact;
   9) **Banking Day** shall mean a day on which the Bank is open for business as required to execute Instructions, with the exception of Saturdays and public holidays;
   10) **Face ID** shall mean a Service User Authentication method using a digital image of the Service User's face stored in his or her mobile phone which has a built-in facial recognition functionality,
   11) **Password** shall, depending on context, mean one of the following terms:
      a) **Access Password**, i.e. the password set up by the Service User upon first signing into the Electronic Banking Service or Telephone Banking Service or upon changing his or her previous Access Password,
      b) **One-Time Password**, i.e. the password provided by the Bank to the Service User to enable him or her to access the Electronic Banking Service or Telephone Banking Service for the first time. The Service User is required to change it for an Access Password upon such first access. A One-Time Password may also be provided on the Service User's Instruction;
      c) **PIN**, i.e. a code defined by the Service User in the Online Banking Service, which the Service User is required to enter to sign into the Mobile Application and authorise Instructions therein;
   12) **Individual Credentials** shall mean individual credentials provided to the Service User by the Bank for authentication purposes;
   13) **Interactive Voice Response**, **or IVR**, shall mean an automated self-service system made available through the Contact Centre to process the Service User's inquiries and Instructions;
   14) **Announcement** shall mean documents which the Bank releases on the Bank Website and makes available from Bank Branches and Post Office Outlets on a regular basis and which contain information on Bank services, including on the types of Time Deposits and Accounts offered by the Bank, the amount of funds which cannot be withdrawn without giving prior

notice to the Bank (notice of Withdrawal), the minimum amounts of Time Deposits and the terms and conditions of adding funds to existing Time Deposits, interest rates applied to deposited funds or overdraft, applicable fees and commissions and rules for charging them, and other information related to the provision of payment services;

15) **Consumer** shall mean a natural person who conducts with the Bank legal transactions which are not directly connected with their business or professional activities;
16) **SMS Code** shall mean a code sent by the Bank to the mobile phone number indicated by the Service User, which must be entered to confirm the Service User's identity and authenticate his or her Instructions;
17) **NBP** shall mean the National Bank of Poland;
18) **CIN** shall mean a Customer Identification Number, i.e. a unique string of eight digits which is assigned by the Bank, which is an element of the Service User Authentication in the Electronic Banking Service and Telephone Banking Service;
19) **Bank Account Number** shall mean a combination of letter and number characters compliant with the NRB standard for domestic payments in Poland or with the IBAN standard for SEPA transfers and other international payment transactions, which unambiguously identifies an Account;
20) **Security Image** shall mean a functionality dedicated to confirming the authenticity of the website used by the Service User to access the Electronic Banking Service as referred to in Clause 5.1 hereof. The Service User is required to select one of a set of Security Images presented to him or her upon first signing into the Electronic Banking Service. The selected Security Image selected is presented to the Service User upon each subsequent signing into the Online Banking Website;
21) **Payee** shall mean a natural person, legal person or unincorporated organisational unit having legal capacity under statute that is the intended recipient of funds transferred in a payment transaction;
22) **Fingerprint** shall mean a Service User Authentication method using the Service User's fingerprint reference data stored in his or her mobile phone which has a built-in fingerprint scanning functionality;
23) **Agent** shall mean a person acting for and on behalf of the Account Holder under a power of attorney;
24) **Bank Branch** shall mean a branch or other retail banking location of the Bank. For a complete list of Bank Branches, including their addresses and opening hours, visit the Bank Website;
25) **Post Office Outlet** shall mean an organizational unit of Poczta Polska S.A. which is contracted by the Bank to perform activities related to concluding Product Agreements and serving Service Users. For a complete list of Post Office Outlets, including their addresses and opening hours, visit the Bank Website;
26) **Payer** shall mean a natural person, legal person or unincorporated organisational unit having legal capacity under statute that places a Payment Order;
27) **BLIK Mobile Payment** shall mean a payment transaction made in PLN using the BLIK Service;
28) **Account Holder or Holder** shall mean a natural person, including a sole trader or a farmer, with whom the Bank has concluded a Product Agreement or, in relation to a joint Account, each of the Joint Account Holders;
29) **Text Message Notification Service** shall mean a service consisting in transmitting notifications concerning a Payment Account by means of text messages;
30) **Account** shall mean an account operated by the Bank for natural persons, including sole traders and farmers, which also serves as a Payment Account as defined in the Payment Services Act. for the types of Accounts operated by the Bank, refer to the Announcement;
31) **Product Terms and Conditions** shall mean product- or service-specific terms and conditions defining a given product or service and governing its delivery and use. In the absence of separate Product Terms and Conditions applicable to a given product or service, the provisions of the relevant Product Agreement shall constitute such Product Terms and Conditions;
32) **Complaint** shall mean a statement made by a Service User to the Bank, whereby such person expresses a grievance about a service or services provided by the Bank;
33) **General Data Protection Regulation (GDPR)** shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th 2016 on the protection of natural

persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

34) **Strong User Authentication** shall mean an authentication that is designed in such a way as to protect the confidentiality of the authentication data and that is based on the use of two or more elements categorised as:
    a) knowledge of something which only the Service User knows,
    b) possession of something which only the Service User possesses, and
    c) and inherence, i.e. something which the Service User is,
    - which are integral to such authentication and which are independent, in that the breach of one does not compromise the reliability of the others;
35) **Bank Website** shall mean the website at www.pocztowy.pl containing information on the Bank's product and service offering, Accounts, Instruction execution terms and conditions, and descriptions of and Service User guidelines for different functionalities available in the Electronic Banking Service and Telephone Banking Service, in particular in the form of demo versions and FAQ documents;
36) **Means of Remote Communication** shall mean means of communication that do not require the simultaneous physical presence of the parties when submitting Instructions, including the telephone, Internet, and mail;
37) **Fees and Commissions Schedule** shall, depending on the context, mean one of the following:
    a) 'Bank Pocztowy S.A. Retail Banking Fees and Commissions Schedule for EnveloBank Products',
    b) 'Bank Pocztowy S.A. Retail Banking Fees and Commissions Schedule',
    c) 'Bank Pocztowy S.A. Retail Banking Fees and Commissions Schedule for Sole Traders and Civil-Law Partnerships'
    d) 'Bank Pocztowy S.A. Retail Banking Fees and Commissions Schedule for Farmers',
    in each case whose full text is available from Bank Branches and Post Office Outlets as well as online on the Bank Website.
38) **Payment Transaction** shall mean an act, initiated by a Payer or a Payee, of placing, transferring or withdrawing funds;
39) **Durable Medium** shall mean any medium which enables the Service User to store information addressed personally thereto in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;
40) **Product Agreement** shall mean an agreement for a product or service, which defines the product or service to be delivered thereunder and governs its delivery and use, in particular the agreement under which the Bank makes available and provides to the User the Electronic Banking Service and Telephone Banking Service;
41) **Unique Service User Profile** shall mean the Service User profile built by the Bank by compiling the Service User's biometric data;
42) **Unique Identifier** shall mean a combination of letters, numbers or symbols specified to the Account Holder by the Bank, including the Bank Account Number, which is provided by the Service User to identify unambiguously another entity and/or his or her Account for a Payment Transaction;
43) **Mobile Device or Mobile Equipment** shall mean a portable electronic device such as a smartphone or tablet, which enables its user to access the Internet, is identifiable by a unique name, has the Mobile Application installed on it, and has been registered and activated by the Service User;
44) **Electronic Banking Service** shall mean a service consisting in providing online access to a Payment Account to enable the Account Holder to check the Account Balance, change cashless payment and debit card transaction limits or submit other Instructions for the Account. As part of the Electronic Banking Service, the Bank provides access to:
    a) the Online Banking Website,
    b) the Mobile Application.
    For the trade names and functionalities of the Online Banking Website and the Mobile Application, refer to the Announcement;
45) **Telephone Banking Service** shall mean a service consisting in providing telephone access to a Payment Account via the Payment Service Provider's dedicated helpline to enable the Account Holder to check the Account Balance or submit other Instructions for the Account.

46) **BLIK Service** shall mean a service allowing the use of a dedicated mobile application to submit PLN-denominated Instructions via the BLIK Mobile Payments System operated by Polski Standard Płatności Sp. z o.o.;
47) **Payment Services Act** shall mean the Polish Payment Services Act of August 19th 2011;
48) **Authentication** shall mean a procedure that enables the Bank to confirm the Service User's identity or the validity of a specific payment instrument, including through the use of Individual Credentials;
49) **Service User** shall mean (i) an Account Holder to whom the Bank has made available the Electronic Banking Service and Telephone Banking Service, (ii) such Account Holder's Agent if the Product Agreement provides for appointment of Agents. and (iii) such Account Holder's legal representative if the Account Holder is a minor over 13 years of age or a partially incapacitated person;
50) **Terms and Conditions** shall mean theses Bank Pocztowy S.A. Electronic and Telephone Banking Terms and Conditions;
51) **Behavioural Biometric Authentication** shall mean a functionality enabling confirmation of the Service User's identity by creating a Unique Service User Profile by recording and analysing the Services User's biometric data, including his or her behavioural characteristics, related to his or her use of the Electronic Banking Service or Telephone Banking Service;
52) **Joint Account Holder** shall mean one of the Holders of a joint Account;
53) **Payment Order** shall mean an Instruction by a Payer or Payee to the Bank, requesting the execution of a payment transaction.

2. Capitalised terms other than those defined above which are used in these Terms and Conditions are defined in the Product Terms and Conditions for the product of service for which the Bank has made available the Electronic Banking Service and Telephone Banking Service. Where the same term is defined differently in these Terms and/or Conditions and in the Product Terms and Conditions, the definition included in these Terms and Conditions shall prevail for the purposes of using the Electronic Banking Service and Telephone Banking Service.

Clause 3

1. If the Product Agreement has been signed with a person other than a consumer, the following provisions of the Payment Services Act shall not be applicable to these Terms and Conditions: all articles of Part II (except Article 32a) and Article 34, Articles 35–37, Article 40.3–4, Article 45, Article 46.2–5, Article 47, Article 48, Article 51 and Articles 144–146.
2. The Service User must not use any of the technological solutions made available to him or her through the Electronic Banking Service or Telephone Banking Service to distribute any illicit content.

Part II. Availability and activation of Electronic and Telephone Banking Services

Clause 4

1. Following execution of the Product Agreement, the Service User may use all or any of the Electronic and Telephone Banking Services.
2. For a complete list of Instructions that can be submitted via the Electronic Banking Service and/or Telephone Banking Service and a description of the system requirements for the use of individual Electronic and Telephone Banking Services, refer to the Announcement.
3. Making the Electronic Banking Service and/or Telephone Banking Service available to a minor over 13 years of age or a partially incapacitated person is subject to prior consent of his or her legal representative to concluding a Product Agreement for such service.

Clause 5

1. The Online Banking Website can be accessed at https://online.pocztowy.pl
2. The Online Banking Website may not operate properly if the Service User has not installed and enabled the most recent version of Java in the web browser he or she uses to access the website. For the list of web browsers recommended for accessing the Online Banking Website, visit the Bank Website.

3. The device that the Service User wishes to use to access the Online Banking Website must enable Internet access and have a properly configured web browser.
4. To use the Online Banking Website and/or Telephone Banking Service, the Service User must provide to the Bank his or her mobile telephone number registered with one of the Polish mobile network operators. Upon being notified by the Service User of a change in his or her mobile phone number, the Bank shall enter the new number in its records as the Service User's mobile phone number to be used for communication between the Bank and the Service User for sending SMS Codes to the latter.
5. Any reference herein to a mobile telephone number shall be a reference to the mobile telephone number which is used by the Service User in the Electronic Banking Service and which may be used in the Telephone Banking Service. Information on the mobile telephone number is available in the Service User's profile in the Electronic Banking Service as well as from Bank Branches and Post Office Outlets.

Clause 6

1. To provide services as part of the Electronic Banking Service, the Bank uses cookies.
2. Cookies are text files that are automatically stored by the Service User's web browser when using the Electronic Banking Service with no effect on the configuration or software of the Service User's device.
3. By enabling the required settings of the software used to access the Electronic Banking Service, the Service User consents to the Bank's use of cookies as referred to in Clause 6.1 hereof.
4. The Service User may at any time object to the Bank's use of cookies and refuse to accept them by changing the relevant settings of his or her web browser, subject to Clause 6.5 hereof.
5. Configuring the web browser that the Service User uses to access the Electronic Banking Service so that it does not accept cookies may prevent proper operation of the Service.
6. For information on how to change the web browser settings, refer to the Bank Website.

Clause 7

1. As part of operating the Electronic Banking Service, the Bank uses session cookies, which enable the Service User to use the Online Banking Website.
2. Session cookies referred to in Clause 7.1 hereof shall be stored on the Service User's device until such time as the Service User signs out of the Electronic Banking Service, leaves the website, or closes the web browser.

Clause 8

The Service User may access the Mobile Application if its has been installed on a mobile device which has been registered and activated and enables Internet access. To use the Mobile Application, the Service User must provide to the Bank his or her mobile telephone number registered with one of the Polish mobile network operators. The provisions of Clause 5.4 hereof on changing the Service User's mobile phone number shall apply mutatis mutandis.

Clause 9

1. The telephone that the Service User wishes to use to access the Telephone Banking Service must enable dual-tone multi-frequency signalling, regardless of whether the Service User's call is to be handled by the IVR or a Contact Centre consultant.
2. The Bank may apply technological solutions that enable automatic call switching between the IVR to Contact Centre consultants. The Service User's call may also be switched at his or her request or if a Contact Centre consultant decides to switch it.

Clause 10

The Service User must activate the Electronic Banking Service and/or Telephone Banking Service prior to its first use.

Clause 11

1. To activate the Electronic Banking Service and/or Telephone Banking Service, upon first signing into the service, the Service User shall:
   1) provide his or her CIN as assigned by the Bank,

2) enter the One-Time Password,
3) select a Security Image (for Online Banking Website only),
4) enter the SMS Code.

2. The Bank shall provide the Service User with a separate One-Time Password for each of the services referred to in Clause 11.1 hereof in accordance with the Instruction received from the Service User:
   1) for the Online Banking Website, the One-Time Password shall be texted at the mobile phone number provided by the Service User and recorded in the Bank's system, which enables text messaging,
   2) for the Telephone Banking Service, the One-Time Password shall be mailed at the Service User's correspondence address or provided in accordance with Clause 11.2.1 hereof.
3. A One-Time Password shall be valid for a limited period of time as indicated in the text message and in the Announcement; upon expiry of that period, the password shall no longer enable signing into the Electronic Banking Service or Telephone Banking Service. In such a case, the Service User should submit an Instruction to receive a new One-Time Password.
4. Upon first signing in, the Service User shall be prompted to set up a proper Access Password in place of the One-Time Password in compliance with the following rules:
   1) for the Online Banking Website:
      a) the Password must be 10–20 characters long,
      b) the password must include at least three of the following four types of characters:
         - a lowercase letter,
         - an uppercase letter,
         - a digit,
         - a special character (for the list of special characters, refer to the Announcement),
      c) no third party should be involved in changing the Password,
      d) the Service User should also ensure that the Internet connection he or she is using when changing the Password is secure in accordance with Clause 18.6 hereof;
   2) for the Telephone Banking Service:
      a) the Password should consist of six digits,
      b) the Password should be changed whenever the IVR so requests,
      c) the Service User may change the Password exclusively by using the dedicated IVR functionality available at the telephone number indicated by the Bank,
      d) no third party should be involved in changing the Password.
5. If upon first signing into the Online Banking Website the Service User fails to change the Password for technical reasons (e.g. Internet connection breakdown), he or she may use the same One-Time Password again to sign into the website.
6. The One-Time Password shall expire on the third failed attempt to sign into the Electronic Banking Service. In such a case, the Service User should submit an Instruction to receive a new One-Time Password.

Clause 12

1. To activate the Mobile Application, the Service User must first install it on his or her mobile device as well as select the right option on the Online Banking Website.
2. To enable the use of the Moblie Application on a mobile device, the Service User may be required to add the Mobile Application publisher to trusted publisher and/or grant certain permissions for the application.
3. After opening the Mobile Application and entering his or her CIN, the Service User will receive an SMS Code which he or she will be prompted to enter in the application.
4. Next, the Service User will be prompted to set a name for the device, which will serve as its identifier on the Online Banking Website.
5. Having completed the above steps, the Service User shall:
   1) sign into the Online Banking Website,
   2) select the command to activate the predefined mobile device in the Mobile Application device management tab,
   3) set up a PIN.
6. The Service User shall comply with the following rules when setting up the PIN:
   1) the PIN must be 5–8 characters long,
   2) the PIN may start with a 0,
   3) the PIN cannot contain a sequence of more than four consecutive digits (e.g. 12345),

4) no digit can be repeated more than three times in a row in the PIN (e.g. 1111).

7. Once the PIN is set up, the Service User shall be required to authorise it by entering an SMS Code sent by the Bank at the mobile telephone number indicated by the Service User.
8. The Service User may activate a limited number of mobile devices. For the maximum number of mobile devices that can be activated, refer to the Announcement.

Part III. Confirming the Service User's identity

Clause 13

1. The Bank shall authenticate the Service User, including by means of Strong User Authentication, upon his or her signing into the Electronic Banking Service or Telephone Banking Service.
2. The Service User shall confirm his or her identity in the Electronic Banking Service or Telephone Banking Service as follows:
   1) when signing into the Online Banking Website or Telephone Banking Service – by providing the correct CIN and Access Password and, if required under applicable laws or regulations, providing additional Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof;
   2) when signing into the Mobile Application – by providing the correct PIN or using the Fingerprint or Face ID Authentication and, if required under applicable laws or regulations, providing additional Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof.
3. Also, to unambiguously confirm the Service User's identity upon accessing the Telephone Banking Service, the Bank may request that the Service User provide additional credentials.
4. To enter the Password in the Electronic Banking Service, the Service User may use the device keypad or a virtual keyboard, as appropriate.

Clause 14

1. If the Service User exceeds the maximum number of failed attempts to provide his or her Individual Credentials in the Electronic Banking Service or Telephone Banking Service, the service shall be blocked. For the number of failed Authentication attempts allowed before the service is blocked, refer to the Announcement. The Service User shall be notified if the service is to blocked. To unblock it, the Service Provider must follow the procedure laid down in Clause 41 hereof.
2. Access to the Mobile Application shall be blocked automatically upon blocking access to the Online Banking Website.
3. The counter of failed Authentication attempts shall be zeroed upon the Service User's first successful attempt to sign into the service which he or she previously failed to sign into.

Clause 15

1. The Bank shall make the Electronic Banking Service and/or Electronic Banking Service available to the Service User under a Product Agreement.
2. Bank products and related services that may be made available under the Product Agreement in accordance with the Bank's offering comprise:
   1) personal bank accounts,
   2) business accounts for sole traders and farmers,
   3) time deposits,
   4) credit facilities,
   5) Payment Cards
   6) other products and services as indicated in the Announcement.
3. The Electronic and/or Telephone Banking Service User who uses more than one of such Bank products and services as are listed in Clause 15.2 hereof shall be assigned a single CIN to access and use all of his or her Bank products and/or services. Even if the Service User uses both Bank products dedicated to consumers and ones dedicated to sole traders or farmers, he or she shall sign into the Electronic Banking Service and/or Telephone Banking Service by providing the same CIN and Password, regardless of the product he or she wishes to use, and, if required

under applicable laws or regulations, by providing additional Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof.

4. Clause 15.4 shall also apply when the Service User is an Agent.

Clause 16

1. The number of active sessions that the Service User can have open at the same time shall be:
   1) on the Online Banking Website – one,
   2) in the Moblie Application – one active session on a single mobile device that has been duly registered and activated.
2. If following signing into the Electronic Banking Service, the Service User does not perform any action for a period of time specified in the Announcement he or she shall be automatically signed out of the service.
3. The Service User shall also be automatically signed out of the Electronic Banking Service if he or she attempts to sign into it again on the same device as that would exceed the number of permitted active sessions under Clause 16.1 hereof.
4. Where Clause 16.2 or 16.3 hereof applies, the system shall display an automatic sign-out message on the Service User's device.
5. The period of time referred to in Clause 16.2 shall run anew each time the Service User opens a new screen on the Online Banking Website or in the Mobile Application.

Part IV. Basic security rules for the Electronic Banking Service and Telephone Banking Service

Clause 17

1. When using the Electronic Banking Service or the Telephone Banking Service, the Service User shall strictly comply with the banking security provisions hereof and any banking security rules published on the Bank Website, as well as follow any other rules and instructions as communicated to him or her in either of the services.
2. The Service User shall promptly notify the Bank if:
   1) he or she learns that his or her Individual Credentials or any other data used by the Service User to confirm his o or her identity or authenticate his or her Instructions in the Electronic Banking Service and/or Telephone Banking Service have been lost, stolen, appropriated or used without authorisation;
   2) he or she learns of an Electronic Banking Service and/or Telephone Banking Service failure or malfunction which may adversely affect the security of the service;
   3) he or she decides to no longer use the mobile phone number he or she has heretofore used for the Electronic Banking Service and/or Telephone Banking Service;
   4) he or she suspects that the Bank Website has been replaced with a fake website.
3. The Service User shall routinely check the date of the most recent Electronic Banking Service sign-in, whether it was successful or failed.
4. If as a result of such check as is referred to in Clause 17.3 hereof the Service User identifies an unauthorised sign-in attempt, he or she shall immediately block access to the Electronic Banking Service and notify the Bank of the situation.

Clause 18

1. The Service User shall memorise the Individual Credentials for the Electronic Banking Service and the Telephone Banking Service and store them with due care.
2. The Bank shall apply the following Authentication methods:
   1) Authentication by means of an SMS Code,
   2) Authentication by means of a Password,
   3) Authentication by means of a PIN entered on a registered and activated mobile device,
   4) behavioural Authentication (provided that the Bank has made such functionality available and is authorised to process the Service User's biometric data under Article 9 of the GDPR),
   5) authentication by means of a Password and SMS Code,

6) combined Password and behavioural Authentication (provided that the Bank has made such functionality available and is authorised to process the Service User's biometric data under Article 9 of the GDPR),
7) Authentication with a Fingerprint scanned using a registered and activated mobile device,
8) Authentication with a Face ID on a registered and activated mobile device (functionality available for iOS devices),
9) Mobile Application authorisation for transactions ordered on the Electronic Banking Website (subject to the availability of such functionality),
10) such other Authentication methods as agreed between the Bank and the Cardholder.

3. The Service User's registered mobile phone number may only be used by the Service User (i.e. it must not be shared with others). The Mobile Application may only be activated on a mobile device that has been registered by the Service User, which is a successful Authentication condition under Clause 18.2.3 hereof.
4. Where permitted by law, the Bank may waive Strong User Authentication.
5. The Bank recommends that the Service User change his or her Access Passwords and PIN for the Electronic Banking Service and Telephone Banking Service at least once a month. The Password and PIN set up by the Service User should comply with the requirements under Clause 11 and Clause 12 hereof, respectively, as well as being difficult to discover by any third parties. The Service User may be prompted to change his or her Password on signing in, subject to Clause 11 and Clause 12 hereof.
6. In order to verify whether the connection with the Online Banking Website is secure, the Service User shall, prior to entering his or her Individual Credentials, check whether the Internet connection is encrypted (padlock symbol) and whether the server certificate is compliant with the requirements specified in the Announcement.
7. The Banks shall also publish information of how to verify whether a connection is secure on the Bank Website.
8. The Electronic Banking Service and/or Telephone Banking Service User shall ensure that any equipment and software he or she uses to access the Electronic Banking Service and/or Telephone Banking Service, as appropriate, satisfies the following requirements:
   1) the Service User's equipment must meet the minimum technical requirements specified by the Bank for the Electronic Banking Service and/or Telephone Banking Service,
   2) the software that the Service User uses to access the Electronic Banking Service and/or Telephone Banking Service, including the operating system, must be up to date and legally licensed,
   3) the Service User's equipment must be protected with antivirus and anti-spyware software, including a firewall, which must be up to date and legally licensed,
   4) the operating system and other software installed on the Service User's equipment must always be up to date in terms of their security features,
   5) the Service User's equipment should be password protected,
   6) the Service User should ensure security of his or her mobile equipment's SIM cards,
   7) the Service User should ensure none of his or her equipment is tampered with in order to bypass security features that protect against unauthorised use of the Electronic Banking Service and/or Telephone Banking Service,
   8) notwithstanding the foregoing, the Service User shall restrict any third-party access to his or her equipment.

Clause 19

1. In order to enable the Service User to check whether there have been any unauthorised attempts to sign into the Electronic Banking Service, the Bank shall provide the Service User with information on Electronic Banking Service sign-ins.
2. Such information as is referred to in Clause 19.1 hereof shall include:
   1) the date and time of the last successful sign-in,
   2) the date and time of the last failed attempt to sign in.
3. If the Service User learns that it was not him or her who last signed, or unsuccessfully attempted to sign, into the Electronic Banking Service, he or she shall:
   1) notify the Bank of such unauthorised sign-in or unauthorised attempt to sign in,
   2) block access to the Electronic Banking Service.
4. The Service User must not disclose to third parties any information on the Authentication methods applied by the Bank or his or her Individual Credentials or any other data used by the Service

User to sign into the Electronic Banking Service and/or Telephone Banking Service. In particular, the Service Provider should exercise caution not to disclose such information or data in response to any email request to do so. The Bank shall never send such email requests to the Service User. Nothing in this Clause 19.4 shall prejudice the Service User's right to use the services of any authorised Third-Party Payment Service Providers.

Clause 20

1. If the Service User learns or suspects that his or her sign-in credentials have been disclosed to any unauthorised third parties, he or she shall change the credentials or block the Electronic Banking Service.
2. The Service Provider shall also promptly notify the Bank if such situation as referred to in Clause 20.1 occurs.
3. The Service Provider shall also submit an Instruction to block the Electronic Banking Service if a situation has arisen which poses, or is likely to pose, a risk to secure storage by the Service User of:
   1) the Service Provider's mobile device,
   2) the Service Provider's Individual Credentials, including his or her Password, Access Password, One-Time Password or PIN,
   3) other information that could enable an unauthorised third party to access the Electronic Banking Service and/or Telephone Banking Service.
4. An Instruction to block the Electronic Banking Service may be submitted:
   1) via the Electronic Banking Service,
   2) via the Telephone Banking Service,
   3) in person at a Bank Branch.

Clause 21

1. The Service Provider must not use an unsecure public network to establish an Internet connection to access the Electronic Banking Service.
2. The Service Provider must not ignore messages displayed by such software as is referred to in Clause 18.8.2–3.

Clause 22

1. The Service Provider may only enter his or her Individual Credentials, including the Password and SMS Codes, and such other credentials as may required to sign into the Online Banking Website or authenticate Instructions thereon at no online address other than the one specified in Clause 5.1 hereof, subject to Clause 22.2 hereof.
2. In order to sign into the Online Banking Website, the Service User shall:
   1) enter the address specified in Clause 5.1 hereof directly in the web browser search bar or
   2) click on the 'sign in' button on the Bank Website.
3. In order to sign into the Online Banking Website, the Service User should not search for the address specified in Clause 5.1 hereof by using any available search engines or click on any links seeming to lead to that website that the Service User may receive in an email. The Bank shall never email the Service User any direct links to the Online Banking Website or requests to provide any credentials for signing into it.
4. This Clause shall not apply to the use by the Service User of services provided by authorised Third-Party Payment Service Providers.

Clause 23

1. Failure by the Service User to comply with the security provisions of this Part IV may:
   1) result in unauthorised interception of the Service User's CIN and Individual Credentials, including sign-in credentials;
   2) cause a breach of the Product Agreement, the Product Terms and Conditions and/or these Terms and Conditions;
   3) constitute grounds for finding the Service User in breach of his or her duty of care;
   4) exempt the Bank from liability or limit its liability towards the Service User.
2. If such failure as is referred to in Clause 23.1 hereof occurs, the Service User may be at risk of losing control of his or her personal data, information on payment transactions executed on the Account, and funds deposited therein.

Clause 24

1. The Bank shall notify the Service User by text message if it enables another Service User to access the former's Bank products and services through the Online Banking Website.
2. The Bank may impose additional restrictions and security requirements on the Service User with respect to access to and use of the Electronic Banking Service and/or Telephone Banking Service if circumstances arise indicating that the security of such access and use may be at risk. The Bank shall notify the Service User if it introduces such additional restrictions or security requirements.

Part V. Liability

Clause 25

1. The Service User shall be liable for any Instructions submitted and payment transactions ordered via the Electronic Banking Service or Telephone Banking Service in accordance with these Terms and Conditions and the specific Product Terms and Conditions covering the Bank product or service which the Instruction is given for.
2. Where the Bank executes an unauthorised payment transaction or fails to execute, or correctly execute, a payment transaction, the Bank shall promptly refund the amount of such payment transaction to the Account on which the Instruction or payment transaction was executed in accordance with the applicable Product Terms and Conditions.
3. Failure to notify the Bank of an unauthorised transaction or a transaction that was not executed or was defectively executed within 13 months from the date the Account was debited with the amount of such transaction shall result in any related claims of the Service User becoming time barred.
4. Clause 25.3 shall not apply if the Bank has failed to provide the Service User with information on such transaction as is referred to in that Clause in accordance with the applicable Product Terms and Conditions.

Clause 26

The Bank shall:

1) keep confidential any data used to confirm the Service User's identity in the Electronic Banking Service or Telephone Banking Service;
2) keep confidential any data used to authenticate payment transactions ordered and Instructions submitted via the Electronic Banking Service and Telephone Banking Service;
3) provide the Service User with access to up-to-date information on the Accounts and Bank products that are available through the Electronic Banking Service and/or Telephone Banking Service.

Part VI. Conclusion of Agreements and submission of Instructions

Clause 27

1. Under the Product Agreement, the Service User and the Bank may use the Electronic Banking Service and/or Telephone Banking Service to submit:
   1) declarations of intent.
   2) assertions of fact.
2. Such submissions as are referred to in Clause 27.1 hereof may relate to banking activities provided for in the applicable Product Terms and Conditions and may be made using relevant functionalities available in the Electronic Banking Service and/or Telephone Banking Service.
3. For information on the scope and types of Agreements that may be concluded or amended via the Electronic Banking Service and/or Telephone Banking Service, refer to the Announcement or visit the Bank Website.
4. To the extent that a declaration of intent requires Authentication, the Service User shall authenticate it in accordance with the applicable provisions of Part VII hereof. The Bank may

require that the Service User provide such additional documents as may be necessary to correctly execute a submitted Instruction; in such a case the Bank shall notify the Service User of such requirement.

5. Conclusion of Agreements based on declarations of intent submitted in electronic form in accordance with these Terms and Conditions shall be subject to the applicable Product Terms and Conditions for Bank products and services for which an Agreement can be so concluded.
6. Declarations of intent submitted via the Electronic Banking Service or Telephone Banking Service shall be deemed to comply with the written form requirement, including where a statute stipulates that a declaration of intent is ineffective unless made in writing, subject to Clause 27.4 and Clause 27.5 hereof.

Clause 28

1. The Bank's communication with the Service User may be in electronic form.
2. Where the Bank sends electronic communication to the Service User as provided for in Clause 28.1 hereof, such communication shall:
   1) be signed with a secure qualified digital signature by a duly authorised representative of the Bank, or
   2) include data enabling identification of the Bank.

Part VII. Submission and Authorisation of Instructions in the Electronic Banking Service and Telephone Banking Service

Clause 29

1. The Service User shall authenticate his or her Instructions as follows:
   1) if the Instruction is submitted on the Online Banking Website:
      a) by accepting the Instruction and, if required under applicable laws or regulations, providing Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof,
      b) by accepting the Instruction if Clause 29.2 hereof applies;
   2) if the Instruction is submitted in the Mobile Application:
      a) by accepting the Instruction and, if required under applicable laws or regulations, providing Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof,
      b) by accepting the Instruction if Clause 29.2 hereof applies;
   3) if the Instruction is submitted via the Telephone Banking Service:
      a) and if such submission is handled by the IVR – by properly signing into the service and accepting the Instruction by pressing the right key on the phone's keypad and, if required under applicable laws or regulations, providing Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof,
      b) and if such submission is handled by a Contact Centre consultant – confirming the data read out by the consultant and, if required under applicable laws or regulations, providing Individual Credentials or using one of the Authentication methods referred to in Clause 18.2 hereof.
2. The Bank may specify Instructions whose execution does not require Authentication using any of the methods referred to in Clause 18.2 hereof. Where the Service User submit such Instruction, confirmation of his or her identity in accordance with Clause 13.2 hereof shall be deemed sufficient to Authenticate the Instruction.
3. By correctly authorising an Instruction, the Service User shall be deemed to have consented to its execution. Such consent may also be given through the Payee, the Payee's Payment Service Provider or an authorised Third-Party Payment Service Provider.
4. This Clause 29 shall apply to Authentication of individual Instructions as well to Authentication of aggregated Instructions submitted using the 'Credit Transfer Basket' functionality.

Clause 30

1. The Bank shall text an SMS Code for authenticating an Instruction to the Service User's mobile telephone number. The SMS Code shall expire after three minutes from its sending.

2. The text message containing an SMS Code shall also include the details of the Instruction to be authenticated therewith as specified in Clause 31 hereof. The SMS Code may only be used to authorise the Instruction for which it was generated.
3. The Service User shall each time check whether the SMS Code he or she receives is intended for the Instruction the Service User wishes to authorise.

Clause 31

1. A text message containing an SMS Code for authenticating a transaction shall also include the following information:
   1) the sender's details,
   2) the daily sequence number of the operation which the Service User instructs the Bank to execute,
   3) the Instruction submission date and time,
   4) the type of the Instruction,
   5) the first two and the last four digits of the Payee's bank account number in the NRB format (in certain cases as indicated on the Bank Website, the Payee's bank account number will be masked),
   6) the amount of the transaction,
   7) the SMS Code to be used to authorise the Instruction.
2. If the SMS Code is to be used to authorise an Instruction other than a payment transaction, the text message shall not include the information specified in Clause 31.1.5–6.

Clause 32

1. If the Service Users enters an incorrect SMS Code to authenticate an Instruction, its Authentication shall require generating a new SMS Code.
2. If the Service User exceeds the maximum number of failed attempts to authenticate an Instruction with an SMS Code, the Bank shall stop sending him or her further SMS Codes and shall block access to the Online Banking Website, of which the Bank shall notify the Service User by displaying a relevant message on the Online Banking Website.

Clause 33

1. Each time the Service User orders a payment transaction, he or she shall check whether the Payee's details, including the Bank Account Number, are correct.
2. Immediately prior to authenticating a payment transaction whose intended Payee is included in the 'Saved Payee List' in the Electronic Banking Service, the Service User shall check whether the Payee's Bank Account Number as presented on the payment transaction summary is correct.
3. Following submission of an Instruction via the Electronic Banking Service or Telephone Banking Service, the Service User shall check whether the Bank has executed it correctly.
4. In the submitted Instruction concerns a payment transaction, such check as is referred to in Clause 33.3 hereof shall consist in:
   1) finding the payment transaction in question in the Account history;
   2) if the payment transaction is a deferred transaction – finding it in the list of scheduled operations and comparing its details with those entered when submitting the Instruction.
5. If the submitted Instruction concerns an operation other than a payment transaction, such check as is referred to in Clause 33.3 shall consist in verifying the status of the request to execute the Instruction.

Clause 34

1. The Bank shall execute payment transactions in accordance with the applicable Payment Account Terms and Conditions.
2. The Terms and Conditions referred to Clause 34.1 hereof also specify the date and time when the Bank is deemed to have received a Payment Order.
3. Information on any executed payment transaction is available in the history of the Account which the transaction was executed on.
4. The Bank shall deliver to the Account Holder, or provide him or her with access to, information on any transactions executed on the Account and any changes in the Account Balance in accordance with the applicable Product Terms and Conditions.

Clause 35

The Bank shall confirm acceptance of an Instruction submitted via the Electronic Banking Service or Telephone Banking Service as follows:

1) if the Instruction is submitted in the Electronic Banking Service – by displaying a relevant system message confirming acceptance of the Instruction for execution or a change in the Electronic Banking Service as requested in the Instruction;
2) if the Instruction is submitted in the Telephone Banking Service:
   a) and if such submission is handled by the IVR – by delivering a relevant voice message,
   b) and if such submission is handled by a Contact Centre consultant – by orally confirming its acceptance

Clause 36

1. To execute a payment transaction ordered by the Service User via the Electronic Banking Service or Telephone Banking Service, the Bank shall rely on the Unique Identifier of the Payer or the Payee, as appropriate.
2. If the Bank refuses to execute a payment transaction, it shall notify the Service User of the refusal, including of the reasons therefor and of the procedure that may be followed to correct any errors that may have caused the refusal, unless giving such notice is prohibited under law.

Clause 37

1. The Service User may cancel a Payment Order until it is received by the Bank.
2. If a Payment Order is initiated through or by an authorised Third-Party Payment Service Provider or the Payee, the Service User may cancel the Payment Order until he or she gives consent to initiating or executing the payment transaction to the provider or the Payee, respectively.
3. A Deferred Payment Order may be cancelled no later than by the end of the Banking Day immediately preceding the agreed execution date of the order.
4. After a relevant time limit as specified in Clause 37.1–3 hereof expires, the Service User may only cancel the Payment Order if agreed with the Bank or Third-Party Payment Service Provider, as appropriate. Execution of Payment Order initiated by or through a Payee shall also be subject to the Payee's prior consent.

Part VIII. Payment transaction amount limits in the Electronic Banking Service and Telephone Banking Service

Clause 38

1. Subject to Clause 38.4 hereof, at the Service User's request, the Bank may apply the following payment transaction amount limits in the Electronic Banking Service for the Service User:
   1) a daily payment transaction amount limit as specified by the Service User,
   2) a single payment transaction amount limit as specified by the Service User up to the daily payment transaction amount.
2. The Account Holder may also request that the Bank apply such limits as are referred to in Clause 38.1 hereof if the Service User is a person authorised to place Payment Orders on behalf of and for the Account Holder.
3. Payment transactions are executed subject to the limits specified in accordance with Clause 38.1 hereof and the Available Balance.
4. The limits referred to in Clause 38.1 hereof shall apply to all of the Service User's Accounts, whether the Account is a personal Account used by the Service User as an individual or a business Account used by the Service User in the capacity of a sole trader or farmer, and shall be defined separately for the Electronic Banking Service.
5. If a transaction is made in a currency other than PLN, in order to determine the amount of the remaining available limit, the Bank shall convert the amount of the transaction at the mid exchange rate quoted by the NBP for the given currency as at the date on which the amount of the remaining available limit is determined. For information on mid exchange rates quoted by the NBP, refer to the Bank Website and/or the NBP website at www.nbp.pl.

6. Deferred payment transactions and payment transactions that have been declined shall decrease the amount of the remaining available daily limit on the day on which they are ordered. If the Service User cancels a deferred payment transaction on the date on which it is ordered, the amount of such cancelled transaction shall increase the amount of the remaining available daily limit.
7. If no such request as is referred to in Clause 38.1–2 hereof is submitted, the only amount limit on payment transactions shall be the Available Balance in the Account.
8. No such amount limit as is referred to in Clause 38.1 hereof shall apply to payment transactions executed under Standing Orders, funds transfers between the Service User's own Accounts held with the Bank, repayments of any credit facilities contracted from the Bank, or the opening of a Time Deposit.
9. The Bank may set up individual amount limits to apply to the Service User, which the Bank shall notify him or her of.
10. The Bank may also set up individual amount limit to apply to certain Instructions submitted by the Service User in the Mobile Application, which the Bank shall notify him or her of.

Part IX. Blocking and unblocking access to the Electronic Banking Service or Telephone Banking Service

Clause 39

1. The Bank shall have the right to block the Service User's access to the Electronic Banking Service and/or Telephone Banking Service for security reasons.
2. Security incidents providing grounds for such blocking as is referred to in Clause 39.1 hereof shall mean situations where a third party has gained, or is likely to gain, unauthorised or otherwise unlawful access to a Bank product or service via the Electronic Banking Service or Telephone Banking Service or other similar incidents as defined in applicable laws or regulations.
3. Prior to blocking the Service User's access to the Electronic Banking Service and/or Telephone Banking Service as provided for in Clause 39.1 hereof, the Bank shall notify the Service User of the situation; where giving such prior notice is not possible, the notice shall be given as soon as practicable after the Service User's access to the service is blocked. The foregoing provision shall not apply where giving such notice could pose a further security risk or is prohibited by law. The Bank shall notify the Account Holder of its refusal to grant a Third-Party Payment Service Provider access to his or her Account in accordance with the applicable Product Terms and Conditions.
4. Subject to Clause 39.3 hereof, the Bank may notify the Service User of blocking his or her access to the Electronic Banking Service or Telephone Banking Service as follows:
   1) by displaying a relevant system message to the Service User upon his or her attempt to sign into the Electronic Banking Service;
   2) by other electronic means, i.e.:
      a) by texting the Service User at his or her phone number,
      b) by email;
   3) by mail;
   4) by giving him or her such notice in person at a Bank Branch or Post Office Outlet,
5. The Bank shall unblock the Service User's access to the blocked service when the reasons for which it was blocked cease to apply.

Clause 40

1. If the Bank learns that the mobile telephone number used by the Service Provider for the Electronic Banking Service and/or Telephone Banking Service is owned by a person other than the Service User, the Bank shall block the latter's access to these services.
2. Where Clause 40.1 applies, the Bank shall also notify the Service User of the fact that it has blocked his or her access to the services.

Clause 41

1. Access to the Electronic Banking Service and/or Telephone Banking Service may be unblocked:
   1) at a Bank Branch,

2) at a Post Office Outlet,
3) by telephone via the Telephone Banking Service if it has not been blocked.

2. Access to the Mobile Application shall not be unblocked automatically upon unblocking access to the Online Banking Website. To unblock access to the Mobile Application, the Service User shall:
   1) if his or her access to the Online Banking Website has been blocked under Clause 14.1 hereof – call the Contact Centre;
   2) if his or her access to the Online Banking Website has been blocked for reasons other than those specified in Clause 14.1 hereof – use the unblocking functionality on the Online Banking Website.

Clause 42

1. If the Service User wishes to send messages to third parties using the solutions available in the Electronic Banking Service and Telephone Banking Service, he or she shall ensure that such third parties acknowledge and agree that they may receive such messages.
2. The Service User must not use any solutions available in the Electronic Banking Service or Telephone Banking Service to distribute any illicit or nuisance content to third parties; engaging by the Service Provider in such distribution may prompt the Bank to block his or her access to those services.
3. If the Service User's access to the Electronic Banking Service and/or Telephone Banking Service as a result of failure to comply with this Clause 42, Clause 39.4 hereof shall apply *mutatis mutandis*.

Clause 43

1. The Service User may request that upon unblocking his or her access to the Electronic Banking Service and/or Telephone Banking Service, the Bank:
   1) not issue a new Password so that the Service User may continue to use his or her existing Password;
   2) issue a One-Time Password to the Service User.
2. Where Clause 43.1.2 applies, a One-Time Password shall be issued on the Service User's Instruction in accordance with the Clause 11.2, Clause 11.3 or Clause 11.4 hereof, as appropriate.

Clause 44

1. In order to block the Mobile Application on a particular mobile device, the Service User may use the device blocking functionality available on the Online Banking Website.
2. Once a mobile device is blocked as provided for in Clause 44.1 hereof, its status on the list of registered mobile devices on the Online Banking Website shall change to 'inactive'.
3. An inactive mobile device may be reactivated in accordance with Clause 12 hereof.

Clause 45

1. The Service User may remove a mobile device from the list of registered mobile devices:
   1) directly in the Mobile Application on the mobile device to be removed, whereupon the Service User shall be automatically signed out of the Mobile Application;
   2) by using the registered device removal functionality available on the Online Banking Website, whereupon the Mobile Application on the removed mobile device shall be deactivated
   3) via the Telephone Banking Service, whereupon the Mobile Application on the removed mobile device shall be deactivated
2. A removed mobile device may be reactivated in accordance with Clause 12 hereof.

Part X. Terms and Conditions of the BLIK Service

Clause 46

1. The Bank shall provide the BLIK Service under Part X hereof and as specified in the Announcement.
2. The BLIK Service enables the Service User to make PLN-denominated BLIK Mobile Payments at points of sale marked with the BLIK symbol, issue and pay with or cash BLIK cheques, and order Credit Transfers to a telephone number, including sending a request for a Credit Transfer or to split a bill (subject to the Bank's making such service available).
3. The Service User may use the BLIK Service on a mobile device if he or she has activated the Mobile Application on that device.
4. The Service User may disable access to the BLIK Service on a mobile device without deactivating the Mobile Application on that device.
5. The BLIK Service requires that the Service User have an Account assigned to BLIK Mobile Payments.
6. The Service User may use the Mobile Application to change the BLIK Service default settings.

Clause 47

1. A BLIK Mobile Payment may be:
   1) a cashless transaction, i.e. a payment for goods or services in PLN, including an online payment,
   2) a cash transaction, including:
      a) a Cash Withdrawal in PLN at an ATM or a Cash Deposit in PLN at a Cash Deposit Machine (subject to the Bank's making such service available),
      b) a Cash Withdrawal in PLN at a BLIK accepting merchant's point of sale offering Cash Withdrawal service,
      c) a Cashback transaction up to the maximum amount specified in the Announcement (subject to the availability of such service).
2. The Service User can make such payments as are referred to in Clause 47.1 hereof using a mobile device or a BLIK Cheque (subject to the Bank's making such service available).
3. When making a BLIK Mobile Payment with a mobile device, the Service User may:
   1) be required to provide a BLIK Code generated in the Mobile Application,
   2) not be required to provide a BLIK Code if the payment is made at a point of sale that the Service User has previously saved as a trusted Payee or using a web browser that the Service User has previously saved a trusted web browser.
4. For the maximum number of active BLIK Cheques that the Service User may generate, refer to the Announcement. Once the maximum number of active BLIK Cheques has been reached, the Service User may only generate another one if one of the already generated ones expires or is removed.
5. When issuing a BLIK Cheque, the Service User shall define its amount, expiration date and PIN.
6. For the maximum amount and longest possible validity period of a BLIK Cheque, refer to the Announcement.
7. A BLIK Cheque may be used by the Service User or a third party. When passing a BLIK Cheque to a third party, the Service User should also provide the right PIN to him or her.
8. If a wrong PIN is entered for a BLIK Cheque three times, the cheque shall be rejected.
9. A BLIK Cheque may be used once up to its amount. If the amount of a transaction paid for with a BLIK Cheque is smaller than the amount of the Blik Cheque, the difference shall be added to the Available Balance in the Account.
10. If the PIN for a BLIK Cheque is lost or forgotten, the BLIK Cheque may be cancelled in the Mobile Application.
11. The Service User may cancel an issued BLIK Cheque in the Mobile Application by removing it from the list of active BLIK Cheques.
12. Upon generation of a BLIK Cheque, the Bank shall place on hold an amount in the Account equal to the amount of the cheque plus the maximum amount of any applicable commission under the Fees and Commissions Schedule.

13. Such hold as is referred to in Clause 47.12 shall be released upon expiry, cancellation or rejection of the BLIK Cheque or upon authorisation of the payment transaction made with the BLIK Cheque.
14. If the Available Balance in the Account is insufficient to cover the amount of a BLIK Mobile Payment plus any fees applicable under the Fees and Commissions Schedule, the transaction shall not be executed.
15. The Bank shall settle such BLIK Mobile Payments as are referred to in Clause 47.1 upon their authorisation.
16. If a BLIK Mobile Payment is not settled upon authorisation, a corresponding amount shall be placed on hold in the Account until the payment is settled.
17. The maximum period of time for which funds can placed on hold shall be determined by the Bank, but in any case cannot be longer than seven calendar days. If the payment is not settled within that time limit, the hold shall be released and the released funds shall increase the Available Balance in the Account.
18. If the payment settles after the Bank releases the corresponding hold, the Bank shall have the right to debit the Account with the amount of the authorised and executed BLIK Mobile Payment plus any commissions applicable under the Fees and Commissions Schedule.
19. Refusal to execute a BLIK Mobile Payment shall be communicated to the Service User upon making such payment in the form a message displayed at the point of sale, ATM or Cash Deposit Machine, as appropriate.
20. The reason(s) for the refusal to execute a BLIK Mobile Payment shall not be communicated to the Service User if such communication is prohibited under law.

Clause 48

1. The BLIK Mobile Payments scheme enables ordering and receiving Credit Transfers where the Payer identifies the Payee solely with the latter's mobile phone number. The party initiating a mobile phone Credit Transfer between two BLIK Service users is the Payee, who sends the Payer a Credit Transfer request via the BLIK Service (a request for Credit Transfer or to split a bill). Requesting splitting a bill consists in sending a request for Credit Transfer to more than two BLIK Service users (subject to the availability of such functionality).
2. In order to be able to receive such Credit Transfers as are referred to in Clause 48.1 hereof, the Service User must register his or her BLIK Alias in the BLIK System, i.e. pair his or her mobile phone number with an Account which the Bank will post transferred funds to.
3. The Service User may register his or her BLIK Alias in the Mobile Application (subject to the availability of such functionality).
4. The Service User may have only one BLIK Alias. An attempt to define another BLIK Alias shall unpair the Service User's mobile phone number from the Account it has been paired with, regardless of whether that Account is held with the Bank or another bank.
5. By defining a BLIK Alias, the Service User shall be deemed to have consented to the Bank providing his or her Bank Account Number to other transaction participants.
6. A request for a mobile phone Credit Transfer shall include the following information:
   1) the Payee's phone number, which can be selected from the mobile device's contacts list or entered in a dedicated box;
   2) the Payee's name, which shall be autofilled with the name assigned to the Payee's phone number in the contacts list of the BLIK Service user's mobile device if the Payee's phone number is selected from that list. The BLIK Service user may change the autofilled name;
   3) the amount to be transferred;
   4) a brief description of the transaction.

Clause 49

1. Depending on the Service User's BLIK Mobile Payment limits, the Service User may authorise and confirm BLIK Mobile Payments using his or her mobile device.
2. The following types of daily Transaction Limits apply to BLIK Mobile Payments:
   1) limits on BLIK Mobile Payments which can be made without authorisation:
      a) the daily limit of the amount of a single transaction which can be made without authorisation (but subject to confirmation on a mobile device),
      b) the daily limit on the number of transactions which can be made without authorisation (but subject to confirmation on a mobile device);
   2) the limit on the total amount of all BLIK Mobile Payments that can be made on a single day.

3. For the details of the daily limits on BLIK Mobile Payments that can be made without authorisation, refer to the Announcement.
4. The Service User may use the Mobile Application to change the limits referred to in Clause 49.2.2 hereof for different types of transactions as specified in the application.

Part XI. Miscellaneous

Clause 50

The Bank may use the Electronic Banking Service to send communication to the Service User.

Clause 51

1. For different banking activities performed as part of the Electronic Banking Service and Telephone Banking Service, the Bank shall charge fees and commissions in accordance with the applicable Fees and Commissions Schedule.
2. The amount or rate of a fee or commission charged for such banking activity as is referred to in Clause 51.1 hereof may be changed in accordance with the applicable Product Terms and Conditions for the product or service which the fee or commission is related to.
3. Notwithstanding the foregoing, the Service User shall bear the costs of Internet access, data transmission and telecommunication services he or she uses at applicable rates charged by their providers.

Clause 52

1. The Electronic Banking Service and Telephone Banking Service shall be available 24 hours a day, 7 days a week, subject to Clause 52.3.
2. The standard time for execution of payment transactions submitted via the Electronic Banking Service shall be Central European Time (CET).
3. The Bank shall have the right to temporarily restrict or utterly take down the Electronic Banking Service and/or Telephone Banking Service, including for maintenance purposes. The Bank shall communicate such temporary restrictions or unavailability to the Service User via Bank Website or the Online Banking Website.

Clause 53

1. The Service User may submit Complaints relating to Bank products and/or services available through the Electronic Banking Service and/or Telephone Banking Service in accordance with the Applicable Product Terms and Conditions.
2. The Bank shall notify the Service User on how his or her Complaint has been decided in accordance with the Applicable Product Terms and Conditions.

Clause 54

1. The language of communication between the Parties during the term of the Product Agreement shall be Polish. The Product Agreement shall be governed by and construed in accordance with the Laws of Poland.
2. Any disputes arising from or in connection with performance of the Product Agreement shall be decided by a competent court in the proper venue as determined in accordance with the Code of Civil Procedure.

Clause 55

1. These Terms and Conditions may be amended for good cause.
2. Any amendments hereto shall be made in accordance with the amendment provisions of the applicable Product Terms and Conditions.
3. Good cause for amending these Terms and Conditions by Bank shall be:
   1) expansion of the Bank's product and/or service offering;
   2) improvements in the Bank's existing products and/or services covered by these Terms and Conditions;

3) discontinuation by the Bank of products and/or services provided under the Product Agreement and covered by these Terms and Conditions due to their unprofitability;
4) amendments to any applicable legislation, issuance of decisions, recommendations, or opinions the NBP, PFSA or other competent authorities, or changes in the construction of applicable legislation by courts, in each case necessitating amendments hereto;
5) a risk to a Bank product or service security;
6) a situation where a third party involved in the provision of a Bank product or service makes a change in the delivery or operation of the product or service or ceases to be involved in its provision, whereby amending these Terms and Conditions is necessary to ensure proper performance of the Product Agreement;
7) technological advancement or changes in the requirements of Payment Service Provider associations, whereby amending these Terms and Conditions is necessary to ensure proper performance of the Product Agreement;
8) change in the name of a Bank product or service.

4. Amendments to these Terms and Conditions within the meaning of this Clause 55 shall not include any stylistic or editorial changes or changes in the Bank's registration data, which do not affect the rights and obligations of the Service User in any way.

Clause 56

1. Amendments to these Terms and Conditions as applicable to Account Holders being individuals other than sole traders or farmers shall be made in accordance with the provisions of Part XXII. *Amendments to these Terms and Conditions* of the 'Bank Pocztowy S.A. Personal Accounts Terms and Conditions', subject to Clause 56.2 hereof.
2. Amendments to these Terms and Conditions as applicable to EnveloBank Account Holders being individuals other than sole traders or farmers shall be made in accordance with the provisions of Part *Amendments to these Terms and Conditions and Revision of Fees, Commissions and Interest Rates*' of the 'EnveloBank Personal Account and Payment Card Terms and Conditions'.
3. Amendments to these Terms and Conditions as applicable to Service Users who are sole traders or farmers shall be made in accordance with the provisions of Part *Amendments to these Terms and Conditions* of (as appropriate):
   1) the 'Bank Pocztowy S.A. Business Account and Payment Card Terms and Conditions for Sole Traders', or
   2) the 'Bank Pocztowy S.A. Business Account and Payment Card Terms and Conditions for Farmers'.

Clause 57

Notwithstanding the provisions of Clause 56 hereof, no amendment hereto prompted by the expansion of Electronic Banking Service and/or Telephone Banking Service functionalities shall require terminating these Terms and Conditions as long as it does not affect the scope of Bank services provided to the Service User through the Electronic Banking Service and/or Telephone Banking Service or the amounts or rates of fees or commissions charged to the Service User for their provision. The Bank shall communicate such amendments in an Announcement.

Clause 58

Provision to the Service User of any third-party services through the Electronic Banking Service, if available, may be subject to concluding a relevant third-party product agreement or accepting applicable third-party terms of service. This provision shall not apply to services provided to the Service User by Authorised Third-Party Payment Service Providers.