

**SPECIFIC TERMS AND CONDITIONS FOR THE PROVISION OF
ELECTRONIC AND TELEPHONE BANKING SERVICES AND FOR
THE SUBMISSION OF STATEMENTS IN PKO BANK POLSKI S.A.**



Bank Polski

Content

Chapter 1. General provisions	2
Chapter 2. Provision of electronic banking service or telephone banking service	3
Chapter 3. Submission of instructions	4
Chapter 4. BLIK transactions	5
Chapter 5. Safety rules	6
Chapter 6. Amendment of the Specific Terms and Conditions	9
Chapter 7. Procedure for reporting and handling complaints	9
Chapter 8. Other provisions	10

Chapter 1. General provisions

§ 1.

1. The Specific Terms and Conditions for the Provision of the Electronic Banking Service and the Mobile Banking Service and the Submission of Statements at PKO Bank Polski S.A., hereinafter referred to as the "Specific Terms and Conditions", specify:
 - 1) the principles of Customer service by the Bank through the electronic banking service and the telephone banking service,
 - 2) the principles of making representations to the Bank,
 - 3) the rules for carrying out and settling BLIK transactions.
2. To the extent not regulated in the Specific Terms and Conditions, the provisions of the respective Agreement shall apply.

§ 2.

1. Terms used in the Specific Terms and Conditions shall be understood to mean:
 - 1) **mobile application** - an element of the electronic banking service in the form of a Bank application, installed by the Customer in the process of its activation on a mobile device, enabling the Customer to operate the products and services made available by the Bank,
 - 2) **authorisation** - consent to the execution of an instruction, via the electronic banking service or telephone banking service, preceded by authentication or strong authentication of the Customer or User,
 - 3) **BLIK cheque** - a service in a mobile application to enable a payment transaction, the use of which requires the use of a BLIK cheque code and a pre-established BLIK cheque password,
 - 4) **instruction** - a declaration of will or knowledge, including a payment instruction, made by a Customer or a User,
 - 5) **payment instruction (payment order)** - an instruction on the basis of which the Bank executes a payment transaction,
 - 6) **business day** - a day from Monday to Friday that is not a public holiday,
 - 7) **password to BLIK cheques** - an individual authentication data in the form of a confidential, numerical string of characters, generated at the Customer's request on the website,
 - 8) **individual authentication data** - individual data provided by the Bank for authentication purposes, which may also be used to give consent in connection with an instruction, including for authorisation purposes,
 - 9) **Customer** - a consumer who has concluded or intends to conclude an Agreement with the Bank,
 - 10) **code to BLIK cheque** - an individual authentication data in the form of a number of digits made available in the mobile application,
 - 11) **BLIK code** - an individual authentication data in the form of a number of digits made available in the mobile application,
 - 12) **Announcement** - information made available to the Customer by the Bank: a) at a branch office, or b) on a website, or c) on an online service, or d) on a mobile application, or e) by correspondence, or f) by e-mail,
 - 13) **mPIN** - an individual authentication data in the form of a confidential numeric character string used within a mobile application,
 - 14) **PKO Bank Polski SA (Bank)** - Powszechna Kasa Oszczędności Bank Polski Spółka Akcyjna with its registered office in Warsaw, at Puławska 15, 02-515 Warsaw, registered in the District Court for the Capital City of Warsaw, in Warsaw, XIII Commercial Division of the National Court Register under KRS no. 0000026438, NIP 525-000-77-38, REGON 016298263, share capital (paid-in capital) PLN 1,250,000,000,
 - 15) **contactless BLIK payment** - a BLIK transaction carried out at a terminal with a contactless reader by placing the mobile device close to the terminal's contactless reader,
 - 16) **the Internet service** - an element of the electronic banking service made available on the website, enabling the Customer to operate the products and services made available by the Bank after authentication,
 - 17) **telephone service** - the Bank's hotline for telephone contact between the Bank and the Customer,
 - 18) **strong authentication** - authentication that protects the confidentiality of data requiring the use of at least two of the individual credentials provided by the Bank belonging to a category:
 - knowledge of something that only the Customer knows about,
 - having something that only the Customer has,
 - the characteristics of the Customer,integral part of this authentication and independent in such a way that a breach of one of these elements does not undermine the credibility of the others,
 - 19) **self-service stand** - a stand made available in selected branches of the Bank, during their opening hours, which makes it possible to submit instructions on one's own, without the participation of a Bank employee,
 - 20) **website** - the Bank's website at www.pkobp.pl,
 - 21) **BLIK system** - a mobile payment system operated by Polski Standard Płatności Sp. z o.o., enabling the execution and settlement of BLIK transactions,
 - 22) **means of remote communication** - a means of remote communication by means of telecommunication connections other than those made available through electronic banking services, which is used for contact between the Bank and the Customer, without the need for the physical presence of a representative of the Bank and the Customer, other than a telephone service; the Bank will inform in the Announcement about the types of means of remote communication used for contact between the Bank and the Customer,
 - 23) **BLIK transaction** - a payment transaction carried out through the BLIK system,
 - 24) **payment transaction** - the deposit, transfer or withdrawal of funds initiated by the Customer or the payee,
 - 25) **contactless BLIK transaction** - a BLIK transaction carried out at a terminal or other device with a contactless reader by placing the mobile device close to the contactless reader,
 - 26) **durable medium** - the medium that enables the Customer to store the information addressed to him in a manner allowing access to it for a period of time adequate for the purposes of its preparation and allowing the reconstruction of the stored information unchanged,
 - 27) **Agreement** - the agreement of a given banking product or service provided, including a brokerage service provided by the Brokerage Office, as an organisational unit of the Bank, providing brokerage services in a separate organisational unit of the Bank, concluded between the Customer and the Bank, including the regulations applicable to such agreement,
 - 28) **electronic device** - a device capable of receiving, processing and sending data, via the Internet, meeting the technical requirements referred to in the Specific Terms and Conditions,
 - 29) **mobile device** - an electronic device that can be freely carried and used anywhere,
 - 30) **electronic banking service** - a service consisting in accessing a payment account via the Internet, enabling one to check the balance of the payment account, change limits for non-cash payments and debit card transactions or submit other types of instructions to the account; additionally, the service includes other services and products not listed above, as long as the Bank enables access to them via an online service, mobile application, ATM or self-service station;
when the electronic banking service is used by the Customer to submit a payment instruction, it is considered to be a payment instrument;

the electronic banking service offered by the Bank (provider) includes:

- a) a web service,
 - b) a mobile application, c) an automatic teller machine, pay-in machine or self-service station,
 - 31) **telephone banking service** - a service consisting in accessing a payment account by telephone via the Bank's call centre, enabling in particular to check the balance of the payment account or submit other instructions to the account; the Bank offers the telephone banking service in the form of a telephone service and by means of remote communication; In addition, the telephone banking service includes other services and products not listed above insofar as the Bank provides access to them via the telephone service and by means of remote communication; in the event that the telephone banking service is used by a Customer to submit a payment instruction, it is considered to be a payment instrument,
 - 32) **optional services** - additional services which may be used through the electronic banking service or telephone banking service and which do not constitute the main object of the provision set out in the Agreement,
 - 33) **brokerage services** - services within the meaning of Article 69, section 2 or 4 of the Act on Trading in Financial Instruments in the scope provided by the Brokerage Office, on the basis of an agreement for the provision of brokerage services which the Customer may conclude with the Brokerage Office,
 - 34) **Act** - the Act of 19 August 2011 on payment services,
 - 35) **authentication** - verification by the Bank of the Customer's identity or the validity of the use of a payment instrument, including the use of individual authentication data,
 - 36) **User** - a natural person authorised by the Customer acting in his or her name and on his or her behalf; in the case of the electronic banking service or the telephone banking service, the User may only be a natural person having full legal capacity,
 - 37) **trusted electronic device** - an electronic device indicated by the Customer together with information from its operating system, including information related to the Internet and the browser used, which can be used for Customer authentication or authorisation.
2. Otherwise, terms used in the Specific Terms and Conditions shall be understood in accordance with the definitions used in the Agreement.
 3. The provisions relating to the Customer shall apply mutatis mutandis to the User, unless the Special Terms and Conditions, the Agreement or the scope of the power of attorney granted provides otherwise.

Chapter 2. Provision of electronic banking service or telephone banking service

§ 3.

1. The Bank shall make available to the Customer the possibility to handle the products and services made available by the Bank, including brokerage services, through the electronic banking service or the telephone banking service, with the condition that the Customer must have active access to the Internet service in order to have access to the mobile application. In the event of a change in the condition under which the mobile application is made available to the Customer for security reasons, the Bank will inform the Customer in an Announcement.
2. The Customer accesses the electronic banking service or the telephone banking service after authentication or strong authentication, if required.
3. In order to use the electronic banking service and the telephone banking service, it is necessary for the Customer to have the appropriate ICT equipment. The Bank does not bear the cost of acquiring and maintaining this equipment.
4. In order to use the website, the Customer must have an electronic device, in particular a computer, telephone or other mobile device with an appropriate operating system and internet browser installed on that device. The operating system and web browser installed on this device must be able to connect to the website via HTTPS with SSL certificate support with SHA-2.
5. The use of the mobile application is subject to its activation on the mobile device used by the Customer and the Customer's possession:
 - 1) appropriate technical equipment, in particular mobile device linked to a mobile telephone number of a mobile phone network operator operating in the Republic of Poland or in one of the countries listed on the website and capable of connecting to the Internet,
 - 2) the software installed on the mobile device necessary to interact with the Bank, in particular the mobile application.
6. Activation of the mobile application on a mobile device may require the Customer to send an SMS message to verify the authenticity of the mobile application and the Customer's mobile phone number associated with his/her mobile device. The Customer is charged for sending SMS messages at the rate of the mobile network operator serving his/her mobile number.
7. The Customer has the option of indicating a trusted electronic device on the website, which fulfils the requirements of the security rules as referred to in § 17 section 7 and section 8. For this purpose, it is necessary for the Customer to submit an instruction and authorise it. The Customer manages the list of all trusted electronic devices on the website.
8. Details of the required equipment referred to in sec. 4, its recommended configuration and software shall be made available by the Bank in an Announcement.
9. The list, scope and description of the products and services made available by the Bank through the electronic banking service or the telephone banking service shall be made available by the Bank in an Announcement.
10. The scope of access to the electronic banking service or the telephone banking service with respect to individual products and services made available by the Bank may be limited, enabled or disabled at the request of the Customer, provided that the Bank allows for such a possibility, subject to sec. 11.
11. The Bank may determine, for security reasons, the scope of access to the electronic banking service or telephone banking service, including to individual functions as well as products or services, on the basis of the information obtained from the Customer referred to in § 17 section 9 or on the basis of the type of individual authentication data used by the Customer or additional security features of the electronic banking service, of which it will inform the Customer in an Announcement.
12. Through the electronic banking service or the telephone banking service, the Customer is entitled to conclude Agreements, including Agreements for the provision of brokerage services by the Brokerage Office, if such a method of concluding them has been made available by the Bank, including the Brokerage Office.
13. Information on the current offer and on the available means of concluding individual Contracts is made available on the website.
14. As of 28 June 2025, the Bank shall make available to the public information on how the service meets the accessibility requirements referred to in Article 32(1) and (2) in conjunction with Article 33(1) of the Act on Ensuring that Business Entities Meet the Accessibility Requirements for Certain Products and Services, in an Announcement on the website.

§ 4.

1. A Customer without legal capacity or with limited legal capacity may use the electronic banking service or telephone banking service, insofar as the Bank provides such a function, with the consent of his legal representative.
2. Upon reaching the age of 13, a Customer with at least limited legal capacity shall obtain limited access to the electronic banking service and the telephone banking service, unless the legal representative objects.
3. Upon reaching the age of 18, a Customer with limited access to the electronic banking service or the telephone banking service, provided that he or she has full legal capacity, shall obtain full access to the electronic banking service and the telephone banking service.
4. A Customer who is a partially incapacitated person shall obtain full access to the electronic banking service or the telephone banking service upon acquiring full legal capacity, as soon as documents confirming this fact are submitted to the Bank.
5. The provisions of sec.1-4 shall not apply to the User.
6. Information on the level of access (full, restricted) to the electronic banking service and the telephone banking service is made available on the website.

Chapter 3. Submission of instructions

§ 5.

1. An instruction permitted by the Bank shall be carried out provided that the Customer gives its consent in one of the ways indicated below, subject to sec. 3 to 8:
 - 1) by affixing a signature in a manner permitted by the Bank,
 - 2) by the Customer entering a sequence of digits from an SMS message sent by the Bank to the Customer's mobile phone number indicated for contacting the Bank,
 - 3) with the use of a payment card, in one of the ways envisaged for consenting to payment card transactions,
 - 4) by authorisation through the electronic banking service or telephone banking service, using individual credentials or using the button to confirm the instruction,
 - 5) by the use of individual credentials or a button confirming the submission of an instruction in a manner permitted by the Bank,
 - 6) by bringing a mobile device with a proximity tag close to a terminal with a proximity reader,
 - 7) by verbal declaration by the Customer in a recorded telephone conversation,
 - 8) in any other manner agreed by the Bank with the Customer.
2. Declarations of will or knowledge made by the Bank that require a signature shall bear:
 - 1) his/her own signature,
 - 2) qualified electronic signature,
 - 3) advanced electronic signature,
 - 4) simple electronic signature,
 - 5) in any other manner agreed by the Bank with the Customer.
3. The Bank shall specify in the Announcement: the date of making available, the scope, the detailed description of the method of giving consent and the instructions that can be executed using the given method of giving consent referred to in sec. 1, as well as the list of establishments making them available.
4. If the Customer has activated the mobile application, the authorisation of the instruction takes place via the mobile application.
5. In the event that the Bank informs the Customer, immediately after the instruction has been submitted, of the need for additional confirmation of the instruction on the telephone service or the Internet service or the mobile application, or in any other manner established by the Bank as part of the authorisation process, the instruction is deemed authorised as soon as it has been confirmed by the Customer.
6. If the instruction referred to in sub-sec. 5 is not confirmed within the time limit specified in the information provided to the Customer when the instruction is submitted, the instruction shall be deemed unauthorised. The Bank shall immediately inform the Customer via the online service or the telephone service or the mobile application of the instructions for which a lack of authorisation has been ascertained.
7. The Bank shall execute the instructions without delay, in accordance with the deadlines set by generally applicable laws, taking into account § 16 section 2.
8. The instruction referred to in sec. 1 shall not be executed by the Bank in the event of:
 - 1) the lack of authority of the person making the instruction,
 - 2) the inconsistency of the signature on the instruction with the specimen signature of the person making the instruction submitted to the Bank, provided that the Bank verifies the consistency of the specimen signature,
 - 3) failure to present a valid identity document or instrument required by the Bank to authenticate the Customer,
 - 4) failure to present or timely sending of documents necessary due to the type of instruction to be given,
 - 5) failure to authenticate the Customer correctly,
 - 6) the absence of a correctly expressed consent, as defined in sec. 1,
 - 7) indicated in the relevant Agreement, insofar as the product or service to which this Agreement relates has been made available through the electronic banking service or telephone banking service,
 - 8) the impossibility of applying financial security measures or where, following the application of financial security measures, there is a risk of money laundering or terrorist financing by the Customer, in particular where it is not possible for the Bank to fully identify the nature and purpose of the Customer's transactions through the Bank,
 - 9) the Bank has a justified suspicion of a breach of security rules by the Customer or of the fraudulent nature of an instruction,
 - 10) the Bank has verified in the register of restrictions of PESEL numbers, kept on the basis of the Act on Population Register, that the Customer's PESEL number is listed as restricted. The Bank provides a list of these instructions in the Announcement.

§ 6.

Instructions and statements referred to in § 5 (2) submitted in accordance with Article 7 of the Banking Act shall comply with the requirements of written form to the extent that they are related to banking activities.

§ 7.

1. The Bank enables payment for goods or services offered by other entities by authorising on the website or mobile application payment transactions related to the purchase of goods or services initiated by the Customer through the websites or applications of merchants with whom the Bank has concluded the relevant agreements.
2. The execution and settlement by the Bank of the payment transaction referred to in sec. 1 shall take place immediately after its authorisation referred to in sec. 1.

§ 8.

1. When responding to enquiries from account information service providers, the Bank shall only provide information about the Customer's payment accounts available online, excluding sensitive payment data. The Bank does not verify the consent given by the Customer to the provider of the account information service.
2. The Bank carries out instructions initiated through the provider of the payment transaction initiation service on the same basis as for other payment instructions. The Bank does not verify the consent given by the Customer to the provider of the payment transaction initiation service.
3. The Bank provides a function for the submission and revocation of consents by the Customer for the purposes of enquiries as part of confirming the availability of an amount on a payment account. The Bank only confirms the availability of the amount, including available funds, when the payment account is available online at the time of the request.
4. Where the Bank, for objectively justified and duly documented reasons relating to unauthorised or illegal access to the payment account by the provider referred to in sec. 1 and section 2, including the unauthorised initiation of a payment transaction, also at the Client's request, refuses the provider providing access to account information or the provider providing the payment transaction initiation service access to the payment accounts, the Bank shall provide the Client with information about this fact via the electronic banking service or the telephone banking service, prior to the refusal of access and, at the latest, immediately after such refusal, but no later than on the business day following the day of such refusal, unless its communication would not be advisable for objectively justified security reasons or is contrary to separate provisions of law.

§ 9.

1. The Customer may submit instructions via the electronic banking service or telephone service 24 hours a day, except during periods of interruption necessary for maintenance, technical repairs or the restoration of the correct functioning of the electronic banking service or telephone service.
2. Instructions submitted by means of remote communication may be submitted by the Customer during the hours specified in the Announcement, excluding any period of interruption required for maintenance, technical repairs or the restoration of remote communication facilities.
3. Information on the occurrence of the interruptions referred to in sec. 1 and sec. 2 shall be available on the website, mobile application or telephone service.

Chapter 4. BLIK Transactions

§ 10.

1. Types of BLIK transactions:
 - 1) initiated using a BLIK code,
 - 2) initiated without using a BLIK code,
 - 3) initiated using a BLIK cheque,
 - 4) BLIK contactless transaction,
 - 5) BLIK mobile transfer, including those carried out in connection with a BLIK transfer request.
2. The Customer authorises BLIK transactions in one of the ways referred to in § 5 section 1 points 4-6.
3. The moment of receipt of a payment order relating to a BLIK transaction is the moment the Bank receives the order.
4. BLIK transactions are settled on the payment account selected by the Customer in the mobile application on the date they are made.
5. BLIK transactions are carried out subject to the limits referred to in § 23.
6. To the extent not regulated in the Specific Terms and Conditions, the settlement of BLIK transactions is carried out in accordance with the rules specified in the relevant Agreement for the payment account selected by the Customer referred to in section 4.
7. The Bank may establish a blockage of funds on the payment account referred to in sec. 4 for unsettled BLIK transactions referred to in sec. 1, points 1-4.
8. The blockage referred to in sec. 7 is cancelled upon settlement of the BLIK transaction or after 7 days from the date of its establishment if the Bank does not receive confirmation of the settlement of this transaction. In case of non-receipt of confirmation of BLIK transaction settlement within 7 days, the Bank may charge the Customer with the amount of this transaction as well as the fees and commissions due at a later date, after receiving a confirmation of the settlement of the BLIK transaction.
9. The Bank shall debit the payment account for the BLIK transaction immediately after the Bank receives the transaction for settlement.
10. To ensure the security of BLIK transactions, the Bank may require the Customer to switch on the location of the mobile device or the Bluetooth function on the mobile device used by the Customer for the duration of such transactions.
11. The Bank provides a detailed description of the functionality of BLIK transactions in the Announcement.

§ 11.

A BLIK transaction initiated using a BLIK code is used to make:

- 1) payments for which such a possibility is provided for and at points and devices marked with the BLIK acceptance sign,
- 2) cash withdrawals at ATMs and other points offering such a service marked with the BLIK acceptance sign,
- 3) Cash deposits at cash deposit machines and other points offering this service, marked with the BLIK acceptance sign.

§ 12.

1. A BLIK transaction initiated without the use of a BLIK code is used to make payments for which this possibility is provided for. This transaction will only be carried out if the Customer has previously agreed in the mobile application to carry out transactions initiated without a BLIK code.
2. The consent referred to in sec. 1 may be withdrawn at any time by the Customer in the mobile application or on the website.
3. In special cases related to security requirements, in spite of the Customer's consent referred to in sec. 1, the Bank may require the BLIK code to be entered or the BLIK transaction to be authorised in the mobile application.

§ 13.

1. Making a BLIK contactless transaction is possible at points bearing the BLIK or Mastercard acceptance mark.
2. The BLIK contactless transaction function is deactivated when the mobile application is activated. The Customer can turn it on or off at any time in the mobile app.
3. A BLIK contactless transaction made in a foreign currency is converted by the Mastercard payment organisation into the Polish currency at the rates applied by the Mastercard payment organisation on the date of the transaction. Information on the exchange rates used by the Mastercard payment organisation is available on the website.
4. The Customer authorises a BLIK contactless transaction by bringing the mobile device close to the terminal's contactless reader or other device.

§ 14.

1. The Bank shall make available within the mobile application the possibility of creating a BLIK cheque specifying the amount and the validity period of the cheque, although the Bank may limit the number of BLIK cheques valid at the same time. Information on the maximum number of BLIK cheques created and valid at the same time is available on the website.
2. Using a BLIK cheque requires the Customer to set up a BLIK cheque password, then create a BLIK cheque code on the mobile application.
3. The execution of a payment transaction using a BLIK cheque requires the use of a BLIK cheque code and a BLIK cheque password by the Customer or a third party enabled by the Customer to use a BLIK cheque. A BLIK cheque can be used once up to the amount indicated by the Customer.
4. As soon as the creation of a BLIK cheque is authorised, a block is set up on the Customer's account for the amount of the BLIK cheque.
5. The blockage referred to in sub-sec. 4 shall expire on the expiry date of the BLIK cheque or upon authorisation of the transaction for which the BLIK cheque was used subject to § 10 sub-sec. 7.
6. In the event of a difference between the actual transaction amount and the amount of the BLIK cheque, the transaction is settled taking the difference into account. The amount of the transaction may not exceed the amount indicated by the Customer.

§ 15.

1. In the case of a BLIK mobile transfer via the mobile application, the Customer is obliged to indicate:
 - 1) the number of the payment account to be debited,
 - 2) the data of the payee as required by the order,
 - 3) the payee's mobile phone number,
 - 4) the amount,
 - 5) title.
2. A BLIK phone transfer, including one carried out in connection with a BLIK transfer request, will be executed provided that the recipient's phone number provided by the Customer is registered with the BLIK system and is linked to the payee's payment account.
3. The Customer can send and receive a BLIK transfer request in the mobile application.
4. The Bank will inform you of the date and scope of the BLIK transfer function made available in connection with the BLIK transfer request in the Announcement.

Chapter 5. Safety rules

§ 16.

1. The Bank monitors Customers' instructions and applies mechanisms to ensure the security of the use of the electronic banking service and the telephone banking service.
2. The Bank, as a result of the monitoring and application of the mechanisms referred to in sec. 1, may, for security reasons, introduce restrictions and additional safeguards in relation to the instructions made through the electronic banking service and the telephone banking service. The Bank will inform the Customer of the introduction of restrictions or additional safeguards in an Announcement or via a telephone service.
3. When establishing an User, the Customer shall inform the User of the rules for using the electronic banking service and the telephone banking service, including the security rules.
4. The Bank records in a permanent way for evidential purposes the instructions given within the electronic banking service, the telephone banking service and on the website.
5. The Customer has access to the history of instructions, information directed by the Bank relating to these instructions and security. The Bank will announce the date and scope of the availability of this function in an Announcement.
6. Recordings of the Customer's conversations with the Bank via the electronic banking service and the telephone banking service are the property of the Bank. The recordings are confidential and may only be used in connection with complaints, investigations, court and administrative proceedings and to the extent necessary to carry out supervision of the Bank's activities to the extent required by generally applicable law. The Bank informs the Customer that calls are being recorded.

§ 17.

1. The Customer is obliged to use the electronic banking service and the telephone banking service in accordance with the Specific Terms and Conditions.
2. The Customer is obliged to use the electronic banking service or the telephone banking service using individual authentication data.
3. Authentication may consist of answering verification questions posed to the Customer by the Bank.
4. The Customer is obliged to maintain the confidentiality of information ensuring the secure use of the electronic banking service or telephone banking service.
5. The Customer is obliged to:
 - 1) securely store individual authentication data, not to transmit, not to access and not to disclose them to third parties, including the BLIK code, except as provided by law, taking into account § 14 section 3,
 - 2) not to use their biometric data for authentication and authorisation on a trusted electronic device or other electronic device where third party biometric data are stored on that device,
 - 3) to use the electronic banking service and the telephone banking service securely, in particular to log in and out securely, to terminate a telephone call, not to use automation applications on electronic devices used to use the electronic banking service or the telephone banking service, not to use applications and other mechanisms that allow data to be stored on such devices and not to log in to the electronic banking service during an active session that allows remote desktop operation by unauthorised persons,
 - 4) check the content of the instruction before each authorisation,
 - 5) familiarise himself with the information addressed to him by the Bank in the electronic banking service, with particular reference to the messages received from the Bank prior to authorisation of the payment transaction,
 - 6) familiarise themselves with the rules on the safe use of the electronic banking service available on the website,
 - 7) make sure that they are in fact in possession of the electronic device (actually in control of the device), before submitting an instruction to add this device to the list of trusted electronic devices.
6. Accessing account information, initiating payment transactions or confirming the availability of an amount on a payment account is done using individual credentials.
7. The Customer is obliged to duly secure the devices and software referred to in § 3 (3-8), which he or she uses to use the electronic banking service or telephone banking service by using:
 - 1) only legal software, its ongoing updating and installation of system patches in accordance with manufacturers' recommendations,
 - 2) up-to-date anti-virus and anti-spam software and firewall,
 - 3) the latest versions of web browsers,
 - 4) passwords to prevent unauthorised access to the electronic device by third parties.
8. The Bank recommends keeping up to date with the information on security rules and a detailed description of the measures to be taken by the Customer to ensure the security of access to the electronic banking service or telephone banking service provided on the website, telephone service, web service and mobile application.
9. The Bank reserves the right to request from the Customer information necessary to establish the Customer's needs and knowledge regarding the use of the electronic banking service and the telephone banking service, in particular in order to take measures to increase the security of the use of these services.
10. If the Customer has doubts regarding the security associated with the authorisation of an instruction, the Customer may request the Bank to provide support with regard to the security of such instruction in the manner set out in § 18(1).
11. The Customer is prohibited from providing unlawful content via the electronic banking service or telephone banking service.
12. The Bank has the right to use electronic mechanisms to check whether there is unsafe software on the electronic device used to use the electronic banking service or whether the Customer or a third party has made changes to the mobile application or to the original software required by the Bank installed on the electronic device in question. Making changes to the mobile application or the software required by the Bank or using unsafe software may result in the risk of an unauthorised person taking control of the electronic device.
13. In order to reduce the risk of unauthorised payment transactions, the Bank reserves the right to use tools to verify the instructions submitted by the Customer, in particular to identify security risks on the basis of answers to questions posed to the Customer by the Bank via the electronic banking service, telephone banking service or at the Bank's outlets.
14. In cases related to security requirements, the Bank verifies the Customer's mobile phone number associated with his/her mobile device.

Failure to link the Customer's mobile number to his/her mobile device may result in the inability to activate the mobile application or in the blocking of all or part of access to the mobile application.

15. Failure by the Customer to log in to the mobile application for at least 6 months from the date of the last login may result, for security reasons, in the need to re-activate the mobile application.
16. Failure to verify or log in as referred to in section 14 and section 15 will result in the inability to receive payments under the BLIK phone transfer service referred to in § 10 section 1 item 5 and § 15.

§ 18.

1. The Customer is obliged to immediately report to the Bank the loss, theft, misappropriation or unauthorised use of individual credentials or a mobile device with a mobile application installed or unauthorised access to the electronic banking service or telephone banking service:
 - 1) by telephone service at the telephone numbers, available 24 hours a day, listed on the website, or
 - 2) at the Bank's outlets, the up-to-date list of which is available on the website, or
 - 3) via a website or mobile application.
2. Immediately upon receipt of the notification referred to in sec. 1, the Bank shall block the use of the electronic banking service or the telephone banking service.
3. In the event of suspected theft, misappropriation, unauthorised use of individual credentials or a mobile device with a mobile application installed, or unauthorised access to the electronic banking service or telephone banking service, the Bank recommends that a report of suspected criminal offence be filed immediately with the law enforcement authorities.
4. The Bank may request from the Customer written confirmation of the occurrence of the events referred to in sec. 1 and an indication of the circumstances under which such events occurred or became known.

§ 19.

1. The Customer shall immediately notify the Bank of any identified unauthorised, non-executed, incorrectly initiated or executed payment transactions in the manner referred to in § 25(1). If the Customer fails to notify the identified unauthorised, non-executed or improperly executed payment transactions within 13 months of the date on which the account was debited or from the date, in which the payment transaction was to be executed, the Customer's claims against the Bank for unauthorised, non-executed or improperly executed payment transactions expire.
2. In the event of the occurrence of an unauthorised payment transaction, the Bank shall be obliged immediately, but no later than by the end of the next business day following the discovery of the unauthorised payment transaction with which the Customer's account was debited or upon receipt of a relevant notification, except where the Bank has reasonable and duly documented grounds to suspect fraud and informs the law enforcement authorities thereof in writing, to refund the amount of the unauthorised payment transaction to the Customer, or to restore the Customer's account to the state it would have been in had the unauthorised payment transaction not taken place, unless the Customer has failed to comply with the notification deadline referred to in sub-sec. 1. With regard to the crediting of an account, the value date may not be later than the date on which the amount is debited.
3. The Customer shall be liable for unauthorised payment transactions, up to an amount equivalent to the PLN 50, converted at the average exchange rate announced by the National Bank of Poland, in force on the day the payment transaction is executed, if the unauthorised payment transaction is the result of:
 - 1) use of a payment instrument lost by the Customer or stolen from the Customer,
 - 2) misappropriation of a payment instrument.
4. The provision of sec. 3 shall not apply where:
 - 1) the Customer was not in a position to ascertain the loss, theft or misappropriation of the payment instrument prior to the execution of the payment transaction, except where the Customer acted intentionally, or
 - 2) the loss of the payment instrument prior to the execution of the payment transaction was caused by an act or omission on the part of the Bank or an entity providing services to it referred to in Article 6(10) of the Act.
5. The Customer shall be liable in full for unauthorised payment transactions if he has wilfully or through wilful or grossly negligent breach of at least one of the obligations referred to in § 17 sections 1-5, section 7 and section 8 and § 18 section 1.
6. Once the notification referred to in § 18 (1) has been made, the Customer shall not be liable for unauthorised payment transactions unless the Customer has caused them intentionally.
7. If the Bank does not provide notification in the manner set out in § 18 (1), the Customer shall not be liable for unauthorised payment transactions unless the Customer has caused them intentionally.
8. Where the Bank does not require strong authentication, the Customer shall not be liable for unauthorised payment transactions unless the Customer acted intentionally.
9. Where the payment instruction is submitted directly by the Customer, the Bank shall be liable for the non-execution or improper execution of the payment transaction, subject to sec. 10 and sec. 20, unless it proves that the account of the payee's supplier has been credited in accordance with the Act. The Bank shall not be liable if the 13-month period referred to in sec. 1 has expired.
10. The Bank's liability for the non-execution or improper execution of a payment transaction is excluded in the event of force majeure or if the non-execution or improper execution of a payment instruction results from other legal provisions.
11. Where the Bank is liable under sec. 9, the Bank shall immediately restore the account to the state it would have been in had the non-execution or improper execution of the payment transaction not occurred. With regard to the crediting of an account, the value date may not be later than the date on which the amount is debited.
12. Where a payment instruction is submitted by the Customer to the provider of the payment transaction initiation service, the Bank shall refund to the Customer the amount of the non-executed or improperly executed payment transaction and, if necessary, restore the Customer's debited account to the state it would have been in had the improper execution not taken place.
13. Where the payment instruction is initiated by or through the payee, if the payee's supplier is not liable for the non-performance or improper performance of the payment transaction in accordance with the Act, the Bank shall be liable, subject to the time limit indicated in sec. 1. The provisions of sec. 10 and sec. 11 shall apply mutatis mutandis to the Bank's liability. The Bank shall not be liable if it proves that the payee's supplier received the amount of the payment transaction in question, even if the payment transaction was made late.
14. The Bank's liability referred to in sec.9 and sec. 13 also includes the fees and commissions charged to the Customer as a result of the non-execution or improper execution of the payment transaction.
15. The Customer is entitled, within a period of 8 weeks from the date on which the account was debited, to apply to the Bank for a refund of the amount of an authorised non-cash payment transaction initiated by or through the payee that has already been executed, if all of the following conditions are met:
 - 1) the exact amount of the payment transaction was not specified at the time of authorisation, and
 - 2) the amount of the payment transaction is higher than the amount the Customer could have expected taking into account the type and value of previous payment transactions, the terms and conditions contained in the account agreement and the relevant circumstances of the case.
16. Upon the Bank's request, the Customer shall be obliged to provide factual circumstances confirming the fulfilment of the conditions referred to in sec. 15. The Customer may not invoke reasons relating to currency exchange if a currency exchange rate has been applied in accordance with the Agreement.
17. Within 10 business days from the date of receipt of the request referred to in sec. 15, the Bank shall either refund the full amount of the

payment transaction to the account or provide a justification for refusing the refund, indicating the authorities to which the Customer may refer the matter if he or she does not agree with the justification provided.

18. The Customer shall not be entitled to the refund referred to in sub-sec. 15 if he/she has given his/her consent to execute the payment transaction directly to the Bank and information on the future payment transaction has been delivered or made available to the Customer by the Bank or the payee, in an agreed manner, at least 4 weeks before the date of execution of the payment instruction.
19. If the unique identifier provided by the Customer is incorrect, the Bank shall not be liable for the non-execution or incorrect execution of a payment instruction under the provisions of the Act, but shall, at the Customer's request, take action to recover the amount of the payment transaction in accordance with the procedure indicated in the Act.
20. In the event that the Bank proves the circumstances referred to in sec. 5 or the fact that the payment transaction was authorised, the Bank is entitled to deduct from the Customer's account the amount which the Bank credited to that account as a result of the notification referred to in sec. 2, of which the Bank will inform the Customer in the manner provided for in § 25, sec. 9.

§ 20.

1. The Customer should provide the Bank with a telephone number and an e-mail address (if necessary for the execution of the Customer's instructions) where the Bank can contact the Customer in order to ensure the security of the use of the electronic banking service and the telephone banking service.
2. The Customer is obliged to notify the Bank immediately of any changes to its own and established Users' personal data and contact details, certifying them in the case of personal data with the relevant documents. Failure to update the telephone number or e-mail address will prevent the Bank from carrying out the Customer's instructions via the electronic banking service or the telephone banking service, provided that the telephone number or e-mail address is necessary to carry out the Customer's instructions.
3. A change of the data referred to in sec. 2 may be submitted by the Customer via the electronic banking service or the telephone banking service, unless the Agreement provides otherwise and the Bank permits such a method of data change.
4. The Bank accepts notifications of data changes from Users as far as they are concerned.

§ 21.

1. The Bank reserves the right to block all or part of access to the electronic banking service or telephone banking service:
 - 1) for legitimate reasons relating to the security of access to and use of those services, including payment instructions made thereunder, or
 - 2) in connection with the Customer's failure to update his or her identification or contact details with the Bank, including a document confirming his or her identity, or failure to provide, at the Bank's request, documents necessary for the Bank to apply the financial security measures set out in the Anti-Money Laundering and Terrorist Financing Act, or
 - 3) in connection with a suspicion of unauthorised use of access to an electronic banking service or a telephone banking service or deliberately causing an unauthorised payment transaction using access to an electronic banking service or a telephone banking service, or
 - 4) in the event of termination of the Agreement by the Bank due to suspicion of the use of the Bank's products or services for criminal activities, or
 - 5) if the Bank has a justified suspicion that an unauthorised person has taken control of the electronic device through which the Customer has access to the electronic banking service or telephone banking service, or
 - 6) use of the electronic banking service or telephone banking service by the Customer in a manner contrary to their nature or socio-economic purpose.
2. In the event that the use of the electronic banking service or telephone banking service is related to the credit made available to the Customer under the Agreement, the Bank reserves the right to block, in whole or in part, access to the electronic banking service or telephone banking service to the extent related to the Customer's use of the credit granted to the Customer, due to an increased risk of the Customer's creditworthiness.
3. The Bank, via the electronic banking service, the telephone banking service or by telephone, shall inform the Customer of the blocking of access to the electronic banking service or telephone banking service prior to the blocking or, if this is not possible, immediately thereafter, unless the provision of such information would be unjustified for security reasons or prohibited by law.
4. The blockage is maintained until the reason for which it was made ceases to exist.
5. The Customer may block access to the electronic banking service or the telephone banking service himself.

§ 22.

1. In the event of suspected or actual fraud or security risks, and the need to confirm an instruction made, the Bank may contact the Customer via secure communication channels:
 - 1) a web service,
 - 2) a mobile application,
 - 3) by telephone.
2. In the event of telephone contact from the Bank, the Customer can verify the identity of the Bank employee on the mobile application or finish the call. If there is any doubt about an automated call from the Bank, the Customer should finish the call.
3. If the Customer identifies a security risk, the Customer may contact the Bank:
 - 1) by telephone service at the telephone numbers, available 24 hours a day, listed on the website, or
 - 2) at the Bank's outlets, the up-to-date list of which is available on the website, or
 - 3) via a website or mobile application.
4. Information on the Bank's contact details is available on the website.

§ 23.

1. The Bank establishes the types and amount of the maximum limits of payment transactions that can be performed:
 - 1) via the mobile app,
 - 2) from the payment account via the online service and the telephone service.
2. Subject to sec. 1, a Customer may, for payment accounts of which he is the holder, set a limit for payment transactions initiated under the payment transaction initiation service, provided that the Bank makes such a possibility available.
3. The Bank establishes the types and amount of default limits for payment transactions:
 - 1) Daily limit on the amount of payment transactions made via the mobile application,
 - 2) A daily limit on the number of payment transactions made via the mobile application,
 - 3) A daily limit on the amount of payment transactions made from the payment account via the online service and the telephone service.
4. After activation of the mobile application by the Customer, the limits referred to in sub-sec. 3(1) and sub-sec. 3(2) shall apply to payment transactions made via the mobile application.
5. The limits referred to in sec. 3 may be amended by the Customer at any time, unless otherwise specified in the relevant Agreement and subject to sec. 9.

6. The amount of the limits referred to in sec. 1 may be individually agreed by the Customer with the Bank, provided that the Bank makes such a possibility available, of which it will inform in the Announcement.
7. The Bank shall inform the Customer of the amount and types of limits referred to in sec. 1 in the Announcement on a durable medium.
8. The Bank shall inform the Customer of the amount and types of limits referred to in sec. 3 in the Announcement.
9. The Bank may change the limits referred to in sub-sec. 3 and 5 where there is a justified risk of a security breach in the use of the electronic banking service and the telephone banking service or as a result of a verification of the payment transaction limits carried out by the Bank. The Bank shall inform the Customer of such change in the Announcement.
10. The change of the limit referred to in sec. 5 shall take place immediately following the submission of such an instruction. For security reasons, the Bank may extend the period between the submission of a limit change instruction by the Customer and its execution, of which it will inform the Customer in the online service or telephone service or mobile application or in an SMS message, indicating the date of execution.

Chapter 6. Amendment of the Detailed Conditions

§ 24.

1. The Bank is entitled to amend the Specific Terms and Conditions in the event of:
 - 1) the introduction of new or the repeal or amendment of generally applicable laws relating to the Specific Terms and Conditions to the extent that they reflect a change in such laws,
 - 2) extending, changing or limiting the functionalities of the services, changing the rules of using the services by the Customer, introducing new services, abandoning certain activities which are the subject of the services provided by the Bank, affecting the provisions of the Specific Terms and Conditions, where the change results from the development of the Bank's offer, while at the same time other available functionalities ensure the proper functioning of the services specified in the Specific Terms and Conditions in accordance with their primary purpose,
 - 3) issuance of court rulings or decisions, recommendations or recommendations of the National Bank of Poland, the Financial Supervision Authority or other public administration bodies relating to the Bank, affecting the provisions of the Specific Terms and Conditions to the extent reflecting the court rulings issued or decisions, recommendations or recommendations of the National Bank of Poland, the Financial Supervision Authority or other public administration bodies,
 - 4) the need for the Bank to rectify clerical errors or make other housekeeping changes, provided that this does not result in an increase in the scope of the Customer's obligations or a reduction in the scope of the Customer's rights.
2. The Bank shall inform the Customer of the changes referred to in sec. 1 on paper or on another durable medium.
3. Information on amendments to the Specific Terms and Conditions shall be provided to the Customer no later than 2 months prior to their proposed effective date, together with the date of their entry into force and information on the legal basis for the amendment and its factual circumstances.
4. In notifying the Bank of the changes, the Bank also states that:
 - 1) The Customer shall have the right, prior to the date of the proposed entry into force of the amendments, to terminate the Agreement to the extent governed by the Specific Terms and Conditions without incurring a fee with effect from the date on which the Customer is informed of the amendment, but no later than the date on which the amendments would have been applied,
 - 2) if, prior to the effective date of the amendments, the Customer does not object to these amendments to the Bank, the Customer shall be deemed to have agreed to them,
 - 3) if the Customer objects to the proposed amendments to the Bank, but does not terminate the Agreement in terms governed by the Specific Terms and Conditions, the Agreement, to the extent governed by the Specific Terms and Conditions, shall terminate on the day preceding the effective date of the proposed amendments, without charge.
5. If, prior to the proposed effective date of the amendments to the Specific Terms and Conditions, the Customer does not give written notice of termination of the Agreement to the extent governed by the Specific Terms and Conditions or does not object, the amendments to the Specific Terms and Conditions shall be deemed to have been accepted and to be effective as of the date specified in the information provided to the Customer by the Bank.

Chapter 7. Mode of reporting and handling of complaints

§ 25.

1. Customers can make complaints about products or services provided by the Bank:
 - 1) in writing - either in person at a branch or by post, or to an electronic delivery address, once it has been created and entered in the electronic address database,
 - 2) orally - by telephone or in person for a record during a visit to a branch,
 - 3) electronically - in the electronic banking service.
2. The current telephone numbers and addresses where the Customer can lodge complaints are given on the website and can also be obtained from the outlets.
3. The complaint should contain the Customer's identification data (first name, surname, PESEL no.), current address data, a description of the objection concerning the products or services provided by the Bank and, if possible, the number of the Customer's bank account, payment card or agreement, or a list of the transactions to which the complaint relates, as well as a description of the manner in which the Customer expects the complaint to be handled.
4. The Bank may ask the Customer to provide additional information or documents if obtaining them is necessary to resolve the complaint.
5. A complaint submitted as soon as the Customer becomes aware of the concerns will facilitate and expedite the Bank's fair handling of the complaint.
6. Upon the Customer's request, the Bank shall confirm in writing or in another manner agreed with the Customer, the fact that the Customer has made a complaint.
7. The Bank shall handle complaints promptly, subject to sec. 8, within a period of no more than 30 days of receipt of the complaint. In particularly complex cases which make it impossible to consider the complaint and respond within the time limit referred to in the preceding sentence, the Bank will inform the Customer of the expected time limit for responding, which may not exceed 60 days from the date of receipt of the complaint. In order for the Bank to comply with the time limits set out in the preceding sentences, it shall be sufficient for the Bank to send its reply before their expiry.
8. The Bank shall respond to the complaint with regard to its rights and obligations under the Payment Services Act within no more than 15 working days of receipt. In particularly complex cases, which make it impossible to consider the complaint and respond within the aforementioned time limit, the Customer will be informed of the expected time limit for responding, which may not exceed 35 working days from the date of receipt of the complaint. In order for the Bank to comply with the time limits set out in the preceding sentences, it shall be sufficient to send a reply before their expiry.
9. Once the complaint has been investigated, subject to sec. 10, the Customer will be informed of the outcome in writing or, if requested by the Customer, by e-mail.
10. The response to the complaint referred to in sub-section 8 will be provided either on paper or, at the request of the Customer, by means of another durable medium, in particular by e-mail.
11. After exhausting the complaint procedure with the Bank, the Customer has the right to settle any disputes out of court before:
 - 1) the Bank Consumer Arbitration, in accordance with the rules available at www.zbp.pl,

- 2) the Financial Ombudsman, in accordance with the procedure indicated at www.rf.gov.pl.
12. The Customer has the right to use the possibility of out-of-court settlement of a dispute concerning an agreement concluded via the Internet, electronic banking service or telephone banking service, through the ODR platform, operating in the countries of the European Union, available at: <http://ec.europa.eu/consumers/odr/>.
13. The Customer has the option of seeking assistance from the relevant District or City Consumer Ombudsman.
14. Irrespective of the complaint procedure described above, the Customer shall at all times have the right to bring an action before the competent ordinary court.
15. All complaints are dealt with by the Bank with the utmost care, thoroughness and as quickly as possible.

§ 26.

1. In the event of a positive complaint regarding a BLIK transaction, the Bank credits the Customer's account with the amount of the payment transaction complained of, plus the commissions and interest charged by the Bank. Recognition takes place on the date of the original debit.
2. If the amount of the advertised transaction referred to in sec. 1 is returned to the Customer's account, by the point where the purchase was made, the Bank has the right to debit the payment account with the amount of the earlier credit resulting from the processing of the complaint.

Chapter 8. Other provisions

§ 27.

Information on the functions provided by the electronic banking service or telephone banking service is given on the website.

§ 28.

1. The Customer may use optional services provided by the Bank as part of the electronic banking service or telephone banking service, subject to the limits referred to in § 23.
2. Information on the optional services provided by the Bank is given in the Announcement.
3. The Bank may discontinue optional services in the event that it is no longer possible to continue to provide them on the existing terms and conditions as a result of a significant change in the terms and conditions or the discontinuation of telecommunications, postal, courier, IT, payment, settlement services necessary for the provision of these services by their suppliers, the withdrawal from operation of IT applications necessary for the provision of optional services, or for other important reasons making it impossible for the Bank to provide these services in accordance with the provisions of law.
4. The Bank shall inform the Customer of the discontinuation of the optional service two months in advance.
5. The Customer may cancel the optional service at any time by submitting an instruction via the electronic banking service or the telephone banking service.

§ 29.

1. The Bank may, through its electronic banking service or telephone banking service, make available to customers the possibility of using third-party services or products.
2. The individual credentials may be used by the Customer to conclude agreements and submit instructions for the use of the services or products referred to in sec. 1, of which the Bank shall inform in an Announcement.

§ 30.

During the term of the Agreement, the Customer shall have the right to request at any time that the provisions of the Agreement, the Specific Terms and Conditions or the information set out in Article 27 of the Act be made available to him in paper form or on another durable medium. The Bank may, with the consent of the Customer, provide these documents and information by posting them on a website or Internet service, provided that the website or Internet service allows access to them for a period of time appropriate to the purposes of providing the information and allows the information provided to be reproduced unchanged.

§ 31.

1. The provisions of the Specific Terms and Conditions shall apply until the date of termination or expiry of the last Agreement, subject to sec. 2.
2. The Bank shall make the information referred to in Article 27, Article 29(1) and (5), Article 31(1) and Article 32(1) of the Act available in an Announcement on a durable medium and upon termination or expiry of the last Agreement.
3. In the absence of provisions in the Agreement concerning the possibility of its termination or dissolution, the Customer may terminate the Agreement with respect to the use of the electronic banking service or the telephone banking service under this Agreement.
4. The period of notice referred to in sec. 3 shall be one month and shall be calculated from the date of delivery of the notice of termination to the Bank. The Parties may agree on a shorter notice period.
5. The Customer shall give the termination notice referred to in sec. 3 in writing.
6. The Bank may terminate the use of the electronic banking service or telephone banking service only for the following valid reasons:
 - 1) the Customer's loss of full legal capacity, insofar as full capacity is required by the Bank to use the electronic banking service or the telephone banking service,
 - 2) related to a reasonable suspicion of a security breach resulting from the Customer's failure to log in to the website, mobile application and telephone service for a period of 1 year, calculated from the date of the last login or the date of conclusion of the Agreement,
 - 3) the Bank's inability to comply with its obligations in applying the financial security measures set out in the AML/CFT Act, in particular:
 - a) failure by the Customer to provide the necessary information or up-to-date documents required under the Bank's financial security measures,
 - b) the Bank's inability to fully identify the nature and purpose of payment transactions made by the Customer through the Bank,
 - 4) the use of the electronic banking service or telephone banking service by the Customer for money laundering or terrorist financing,
 - 5) a reasonable suspicion is obtained that the electronic banking service or the telephone banking service is used for other offences than those specified in sec. 4,
 - 6) the Customer's provision of untruths or concealment of the truth with regard to the information that the Customer is obliged to provide to the Bank, as an entity providing an electronic banking service or a telephone banking service, in accordance with the regulations,
 - 7) the use of the electronic banking service or telephone banking service by the Customer in a manner contrary to their nature or socio-economic purpose, including the use of the electronic banking service or telephone banking service to carry out settlements related to the conduct of business or profit-making activities,
 - 8) the inability of the Bank to continue to provide the electronic banking service or the telephone banking service on the existing terms and conditions, as a result of a significant change in the terms and conditions or the discontinuation of the provision of telecommunications, postal, courier, IT, payment, settlement services necessary for the provision of these services by their suppliers, the withdrawal from the operation of the IT applications necessary for the provision of the electronic banking service or the telephone banking service, or for other valid reasons preventing the Bank from providing the electronic banking service or the telephone banking service in accordance with the law.

7. The Bank reserves the right to terminate the Agreement with respect to the use of the electronic banking service or the telephone banking service under this Agreement in the event that the Customer is subject to national or international sanctions or embargoes established by Poland, the European Union, the United Nations in connection with the performance of obligations under anti-money laundering and terrorist financing legislation or sanctions.
8. In the cases referred to in sec. 6, the period of notice shall be two months and shall be calculated from the day following the day on which the Bank serves notice of termination on the Customer.
9. The Bank shall terminate the electronic banking service or telephone banking service in writing, stating the reasons for the termination.

§ 32.

1. The public administration body supervising the Bank's activities is the Financial Supervision Commission.
2. The customer may lodge a complaint with the Financial Supervisory Commission against the Bank's activities if these activities violate the law.
3. The generally applicable provisions of law shall apply to the determination of the competent court for the resolution of disputes arising from the provision of the electronic banking service or telephone banking service by the Bank and from the submission of statements by Customers.
4. The governing language for matters covered by the Specific Terms and Conditions is Polish.