The amendments to the relevant documents are presented in the table below.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Clarification of definitions related to the Payment Services Act of 19 August 2011 (Journal of Laws 2011, No 199, item 1175)	
Pre-amendment wording	**Post-amendment wording**
§ 1.2. Interactive Voice Responder – a free-of-charge CitiPhone functionality that enables the user to obtain information and to execute, without a consultant's involvement, some operations using the Card number along with the CitiPhone PIN and an Authorization Code or with the use of the CitiPhone PIN only if the Customer has an active Incoming Call Identification Service, or using Mobile Authentication;	§ 1.2. Interactive Voice Responder – a free-of-charge CitiPhone functionality that enables the user to obtain information and to execute, without a consultant's involvement, some operations using the Card number along with the CitiPhone PIN and an Authentication Code or with the use of the CitiPhone PIN only if the Customer has an active Incoming Call Identification Service, or using Mobile Authentication;
§ 1.3. Transaction Authorization – consent by the Customer/User to execute a Transaction in the form and under the procedure provided for in these Terms and Conditions, preceded by Authentication or Strong Authentication.	§ 1.3. Transaction Authorization – consent by the Customer/Authorized User to execute a Transaction in the form and under the procedure provided for in these Terms and Conditions, preceded by Authentication or Strong Authentication.
§ 1.12. CVV2/CVC2 – a three-digit number placed on the Card or, in the case of a Virtual Card in Citi Mobile, used to authorize Transactions when making a payment without the Card's physical use.	§ 1.12. CVV2/CVC2 – a three-digit number placed on the Card or, in the case of a Virtual Card in Citi Mobile, used for the Authentication of Transactions when making a payment without the Card's physical use.
§ 1.24. Payment Instrument – a personalized device or set of procedures used by the Customer to submit a Payment Instruction, in particular a Card, Citibank Online, Citi Mobile, CitiPhone Telephone Banking Service.	§ 1.24. Payment Instrument – a personalized device or a set of procedures agreed between the Customer and the payment services provider used for initiating a Payment Instruction, in particular a Card, Citibank Online, Citi Mobile, CitiPhone Telephone Banking Service.
§ 1.30. Authorization Code – a one-time code generated by the Bank, used for Authentication, including Strong Authentication, of Transactions or operations carried out by the Customer/User in Citibank Online, Citi Mobile, CitiPhone phone banking service, at a Branch or on the Internet.	deleted and replaced with the term Authentication Code
none	§ 1.29. Authentication Code – a one-time code generated by the Bank, used for Authentication, including Strong Authentication, of Transactions or operations carried out by the Customer/Authorized User in Citibank Online, Citi Mobile, CitiPhone, at a Branch or on the Internet (to the extent permitted for these services).
§ 1.31. BLIK Code – a string of digits generated via Citi Mobile for making BLIK Transactions.	§ 1.30. BLIK Code – a string of digits generated via Citi Mobile for Authenticating BLIK Transactions.
§ 1.53. PIN – a personal confidential Identification Code of the Customer/User enabling the execution of Transactions.	§ 1.52. PIN – a confidential personal Customer/Authorized User Identification Code used for Authenticating Transactions.
§ 1.54. Citi Mobile Token PIN – a confidential six-digit Customer/User identification number used for Authentication, including Strong Authentication, with the use of a Citi Mobile Token.	§ 1.53. Citi Mobile Token PIN – a confidential six-digit Customer/Authorized User identification number used for Authentication, including Strong Authentication, with the use of a Citi Mobile Token.

§ 1.56. Payer – a natural person, a legal person or an organizational unit without legal personality having legal capacity under statutory law, that submits a Payment Instruction (Customer/User).	§ 1.55. Payer – a natural person, a legal person or an organizational unit without legal personality having legal capacity under statutory law, that submits a Payment Instruction (Customer/Authorized User).
§ 1.79. Strong Authentication – authentication that ensures the protection of data confidentiality by using at least two elements from the following categories: – something only the user knows; – something only the user has; – something the user is (user's characteristic features); incorporated into such authentication and independent of one another so that compromising one of those elements will not undermine the reliability of the other elements.	§ 1.78. Strong Authentication – Authentication that ensures the protection of data confidentiality by using at least two elements from the following categories: – something only the Customer/Authorized User knows; – something only the Customer/Authorized User has; – something the Customer/Authorized User is (Customer's/Authorized User's characteristic features); incorporated into such authentication and independent of one another so that compromising one of those elements will not undermine the reliability of the other elements.
§ 1.80. Preparation of a summary of payment transactions – a service initiated by the Payer, consisting in a summary of payment account transactions being prepared by the entity that maintains the payment account; the statement is prepared in paper or electronic format.	§ 1.79. Preparation of a summary of Transactions – a service initiated by the Payer, consisting in a summary of payment account transactions being prepared by the entity that maintains the payment account; the statement is prepared in paper or electronic format.
§ 1.97. Citibank Online Authentication – authentication of Special Transactions or Cashless Transactions carried out without physical use of the Card via the Internet, involving electronic identification of the Customer/User in Citibank Online through entering the User Name and the Identification Code.	§ 1.97. Citibank Online Authentication – Authentication of Special Transactions or Cashless Transactions carried out without physical use of the Card via the Internet, involving electronic identification of the Customer/Authorized User in Citibank Online through entering the User Name and the Identification Code.
§ 1.29. Customer – a person having full capacity for legal transactions, who has entered into an Agreement with the Bank and carries out Transactions in their name and for their benefit for a purpose not directly connected with their business or professional activity, who is a consumer within the meaning of Article 22 of the Civil Code Act of 23 April 1964 (hereinafter the 'Civil Code') and who is the holder of a Primary Card.	§ 1.98. User/Customer – a natural person having full capacity for legal transactions, who has entered into an Agreement with the Bank and carries out Transactions in their name and for their benefit for a purpose not directly connected with their business or professional activity, who is a consumer within the meaning of Article 22 of the Civil Code Act of 23 April 1964 (hereinafter the 'Civil Code') and who is the holder of a Primary Card.

Terms and Conditions of Citibank Credit Cards

In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of:

(b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.

Factual background behind the amendment: Need to align definitions to the current status of relevant functionalities

Pre-amendment wording	Post-amendment wording
§ 1.19. ePIN – the Customer's/User's personal, confidential Identification Code used in the 3D Secure Authentication procedure, which allows for Transactions to be made via the Internet without physical use of the Card. Until the Customer/User independently assigns an ePIN, the ePIN is the same as the Card PIN, but no longer than until 09/05/2023 or the fifth use of the Card PIN in the 3D Secure Authentication procedure, whichever comes first.	§ 1.19. ePIN – the Customer's/Authorized User's personal, confidential Identification Code used in the 3D Secure Authentication procedure, which allows for Transactions to be made via the Internet without physical use of the Card.
§ 1.11. Cookies – files storing information or providing access to information already stored in a terminal telecommunications device during or after visiting websites, including websites of the Bank.	§ 1.11. Cookies – files storing information or providing access to information already stored in the terminal telecommunications device used by the End User for accessing Citibank Online.

§ 1.74. Card Account – a technical PLN-denominated account maintained with the Bank where the Transactions made and fees, commissions and interest due to the Bank under the Agreement as well as the Outstanding Balance payments are posted. A Card Account is attached to a specific Card. The Bank opens a Card Account upon issuing a Primary Card or a Supplementary Card. The Card Account may be changed if the Card is replaced in any of the situations described in § 4.4. and § 4.5. The Card Account assigned to the Primary Card is always shown in the Statement and accessible via Citibank Online or Citi Mobile.	§ 1.73. Card Account – a technical PLN-denominated account maintained with the Bank where the Transactions made and fees, commissions and interest due to the Bank under the Agreement as well as the repayment of Outstanding Balance are posted. A Card Account is attached to a specific Card. The Bank opens a Card Account upon issuing a Primary Card or a Supplementary Card. The Card Account may be changed if the Card is replaced in any of the situations described in § 4.4. and § 4.5. The Card Account assigned to the Primary Card is always shown in the Statement, except when the Card Account has been closed and there is an overpayment on it, and is accessible via Citibank Online or Citi Mobile.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.	
Factual background behind the amendment: Need to change the defined term with no revision of the definition text	
Pre-amendment wording	**Post-amendment wording**
§ 1.98. User – a Supplementary Card user authorized by the Customer to make Transactions in the Customer's name and for the Customer's benefit using the Supplementary Card.	§ 1.89. Authorized User – a Supplementary Card user authorized by the Customer to make Transactions in the Customer's name and for the Customer's benefit using the Supplementary Card.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.	
Factual background behind the amendment: Revision of the wording further to the change of the defined term from User to Authorized User, amendment introduced in order to add clarity	
Pre-amendment wording	**Post-amendment wording**
§ 1.10. CitiPhone PIN – a Customer's/User's identification code used for the verification of their identity via the CitiPhone Telephone Banking Service and for executing banking cash settlements using the CitiPhone Telephone Banking Service, assigned independently by the Customer/User and known only to the Customer/User.	§ 1.10. CitiPhone PIN – a Customer's/Authorized User's identification code used for the verification of their identity via the CitiPhone Telephone Banking Service and for executing banking cash settlements using the CitiPhone Telephone Banking Service, assigned independently by the Customer/Authorized User and known only to the Customer/Authorized User.
§ 1.14. Personal Data – personal data within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation), pertaining to the Customer/User.	§ 1.14. Personal Data – personal data within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation), pertaining to the Customer/Authorized User.

§ 1.16. Third Party Provider – a payment services provider, other than the Bank, that renders one or more of the following services in accordance with the Payment Services Act: – initiation of a payment transaction whereby the provider initiates a Payment Instruction from the Card Account on request of the Customer/User; – access to account information, consisting in online delivery by such provider of consolidated information on the Card Account or Card Accounts maintained by the Bank or payment accounts maintained by providers other than the Bank; or – issue of payment card-based payment instruments, consisting of issuing by such provider of payment card-based payment instruments to enable the user to make payment transactions;	§ 1.16. Third Party Provider – a payment services provider, other than the Bank, that renders one or more of the following services in accordance with the Payment Services Act: – initiation of a payment transaction whereby such a provider initiates a Payment Instruction from the Card Account on request of the Customer/Authorized User; – access to account information, consisting in online delivery by such provider of consolidated information on the Card Account or Card Accounts maintained by the Bank or payment accounts maintained by providers other than the Bank; or –- issue of payment card based payment instruments, consisting in issuing payment card based payment instruments by such provider to enable the User to make payment transactions;
§ 1.38. Supplementary Card Credit Limit – the maximum amount of an authorized Outstanding Balance denominated in Polish zlotys (PLN) and established individually for the User by the Bank at the Customer's request, within the scope of the Credit Limit.	§ 1.37. Supplementary Card Credit Limit – the maximum amount of authorized Outstanding Balance denominated in Polish zlotys (PLN) and established individually for each Authorized User by the Bank at the Customer's request subject to the Credit Limit.
§ 1.40. Biometric Method – Customer/User identity verification on a Mobile Device consisting in checking the Customer's/User's characteristic features (a fingerprint, iris or face map) using an appropriate functionality available on the Mobile Device;	§ 1.39. Biometric Method – Customer/Authorized User identity verification on a Mobile Device consisting in checking the Customer's/Authorized User's characteristic features (a fingerprint, iris or face map) using an appropriate functionality available on the Mobile Device;
§ 1.41. Mobile Device Unlocking Method – a method for unlocking a Mobile Device based on the Customer's/User's knowledge.	§ 1.40. Mobile Device Unlocking Method – a Mobile Device unlocking method based on the Customer's/Authorized User's knowledge.
§ 1.43. User Name – a name assigned by the Customer/User which defines them as a user in the Citibank Online service, in Citi Mobile, and is used for the purpose of logging into that service.	§ 1.42. User Name – a name assigned by the Customer/Authorized User which defines them as a user in Citibank Online or in Citi Mobile, and is used for the purpose of logging in to that service.
§ 1.51. Pay by Link (Płacę z Citi Handlowy) – an automated online payment made from a Card Account based on an internal transfer order in PLN or a domestic transfer order in PLN via an Online Payments Operator selected by the Customer/User. Pay by Link (Płacę z Citi Handlowy) is not a payment executed by a Third Party Provider.	§ 1.50. Pay by Link (Płacę z Citi Handlowy) – an automated online payment made from a Card Account based on an internal transfer order in PLN or a domestic transfer order in PLN via an Online Payments Operator selected by the Customer/Authorized User. Pay by Link (Płacę z Citi Handlowy) is not a payment executed by a Third Party Provider.
§ 1.92. Incoming Call Identification Service – a function for identifying a Customer/User who is making a call under the CitiPhone Telephone Banking Service using a Primary Mobile Phone; such identification is carried out on the basis of the mobile phone number used by the Customer/User, and notified previously to the Bank, and the CitiPhone PIN.	§ 1.92. Incoming Call Identification Service – a function for identifying a Customer/Authorized User who is making a call under the CitiPhone Telephone Banking Service using a Primary Mobile Phone; such identification is carried out on the basis of the mobile phone number used by the Customer/Authorized User, and notified previously to the Bank, and the CitiPhone PIN.
§ 1.94. Authentication – a procedure enabling the Bank to verify the Customer's/User's identity or validity of use of a specific payment instrument, including the use of individual authentication data;	§ 1.94. Authentication – a procedure enabling the Bank to verify the Customer's/Authorized User's identity or validity of use of a specific payment instrument, including the use of individual authentication data;
§ 1.95. 3D Secure Authentication/3D Secure – a method of authentication of Transactions made without the physical use of the Card via the Internet, consisting in the Customer/User entering the 3D Secure Password (Visa – under the name 'Verified by Visa', MasterCard – under the name 'MasterCard SecureCode') received to the Primary Mobile Phone Number and ePIN.	§ 1.95. 3D Secure Authentication/3D Secure – a method of Authentication of Transactions made without the physical use of the Card via the Internet, consisting in the Customer/Authorized User entering the 3D Secure Password (Visa – under the name 'Verified by Visa', MasterCard – under the name 'MasterCard SecureCode') received to the Primary Mobile Phone Number and ePIN.
§ 1.99. End User – a Customer using Citibank Online or requesting the provision of the Citibank Online service and a Customer using the CitiPhone Telephone Banking Service or requesting the provision of the CitiPhone Telephone Banking Service.	§ 1.99. End User – a Customer/Authorized User using Citibank Online or requesting the provision of the Citibank Online service and a Customer/Authorized User using the CitiPhone Telephone Banking Service or requesting the provision of the CitiPhone Telephone Banking Service.
§ 1.111. Payment Instruction – a statement made by the Customer/User or Recipient to the Bank, containing an order to initiate or carry out a Transaction or to make a Deposit into the Card Account.	§ 1.111. Payment Instruction – a statement made by the Customer/Authorized User or Recipient to the Bank, containing an order to initiate or carry out a Transaction or to make a Deposit into the Card Account.

§ 2.9. The provisions of these Terms and Conditions and of the Agreement referring to the Customer shall apply to the User/Attorney, as relevant, save that, in relations between the Bank and the Customer, the Customer shall be financially liable to the Bank for any of the User's/Attorney's acts related to the use of the Supplementary Card.	§ 2.9. The provisions of these Terms and Conditions and of the Agreement referring to the Customer shall apply to the Authorized User/Attorney, as relevant, save that, in relations between the Bank and the Customer, the Customer shall be financially liable to the Bank for any of the Authorized User's/Attorney's acts related to the use of the Supplementary Card.
§ 4.6. Any change of the type of the Customer's Card will result in the change of the type of the Cards issued to the Users and the replacement of Contactless Media issued to the Card.	§ 4.6. Any change of the type of the Customer's Card will result in the change of the type of the Cards issued to the Authorized Users and the replacement of Contactless Media issued to the Card.
§ 5 1. Upon the Customer's application, the Bank may issue payment cards – Supplementary Cards to Users designated by the Customer. 2. Promptly upon receiving the Supplementary Card in the form of a physical card, the User shall sign the Card permanently, activate the Card and define the PIN and ePIN. The Customer may activate the Supplementary Card and assign the PIN via Citibank Online or Interactive Voice Responder. The User may activate the Supplementary Card and assign the ePIN via Citibank Online or Citi Mobile. 3. The Customer will be liable for any Transactions made with Supplementary Cards and for any overrun of the Supplementary Card Credit Limit by a User. The Customer can request the Bank at any time to change the Supplementary Card Credit Limit within the Credit Limit. An instruction to change the Supplementary Card Credit Limit may be submitted by the Customer at a Branch, via Citibank Online or the CitiPhone Telephone Banking Service, and it will be effective, at the latest, on the following Business Day unless the actually utilized Supplementary Card Credit Limit is higher than the Limit applied for by the Customer. Any Transactions made with Supplementary Cards shall be debited to the Primary Card Account and to the Credit Limit. 4. A Supplementary Card has a technical Card Account separate from the Primary Card, but any Deposits made into this account repay the Outstanding Balance. 5. On the Customer's application, the Bank may provide the Customer/User with a Contactless Medium linked to the Card for making Contactless Transactions. Promptly upon receiving such Contactless Medium, the Customer/User shall assign a PIN and activate the Contactless Medium. The Supplementary Card User may activate the Contactless Medium and define the PIN via Citibank Online or Interactive Voice Responder. 6. The Supplementary Card and the Contactless Medium may be used exclusively after their activation, during the term of the Primary Card Agreement, on the terms and conditions laid down therein. A Supplementary Card and/or a Contactless Medium will lose their validity upon Agreement termination. 7. Insofar as not specified above, the Terms and Conditions applicable to the Card shall apply to the Contactless Medium. 8. The Customer/User may opt out of the Supplementary Card or the Contactless Medium at any time.	§ 5 1. Upon the Customer's application, the Bank may issue payment cards known as Supplementary Cards to Authorized Users named by the Customer. 2. Promptly upon receiving the Supplementary Card in the form of a physical card, the Authorized User shall sign the Card permanently, activate the Card and define the PIN and ePIN. The Customer may activate the Supplementary Card and assign the PIN via Citibank Online or Interactive Voice Responder. An Authorized User may activate the Supplementary Card and assign an ePIN via Citibank Online or Citi Mobile. 3. The Customer will be liable for any Transactions made with Supplementary Cards and for any overrun of the Supplementary Card Credit Limit by an Authorized User. The Customer can request the Bank at any time to change the Supplementary Card Credit Limit within the Credit Limit. An instruction to change the Supplementary Card Credit Limit may be submitted by the Customer at a Branch, via Citibank Online or the CitiPhone Telephone Banking Service, and it will be effective, at the latest, on the following Business Day unless the actually utilized Supplementary Card Credit Limit is higher than the Limit applied for by the Customer. Any Transactions made with Supplementary Cards shall be debited to the Primary Card Account and to the Credit Limit. 4. A Supplementary Card has a technical Card Account separate from the Primary Card, but any Deposits made into this account repay the Outstanding Balance. 5. On the Customer's application, the Bank may provide the Customer/Authorized User with a Contactless Medium linked to the Card for making Contactless Transactions. Promptly upon receiving such Contactless Medium, the Customer/Authorized User shall assign a PIN and activate the Contactless Medium. The Authorized User of the Supplementary Card may activate the Contactless Medium and assign the PIN via Citibank Online or Interactive Voice Responder. 6. The Supplementary Card and the Contactless Medium may be used exclusively after their activation, during the term of the Primary Card Agreement, on the terms and conditions laid down therein. A Supplementary Card and/or a Contactless Medium will lose their validity upon Agreement termination. 7. Insofar as not specified above, the Terms and Conditions applicable to the Card shall apply to the Contactless Medium. 8. The Customer/Authorized User may opt out of the Supplementary Card or the Contactless Medium at any time.
§ 6.2. The Card shall expire: (a) upon the expiry of its validity period (upon the lapse of the last day of the month indicated on the Card); (b) due to blocking; (c) when exchanged for a new Card;	§ 6.2. The Card shall expire: (a) upon the expiry of its validity period (upon the lapse of the last day of the month indicated on the Card); (b) due to blocking; (c) when exchanged for a new Card;

(d) in the event of death of the Customer – with regard to the Primary Card and Supplementary Card, and in the event of death of a User – with regard to a Supplementary Card, expiration, termination or withdrawal from the Agreement,	(d) in the event of death of the Customer – with regard to the Primary Card and Supplementary Card, and in the event of death of an Authorized User – with regard to a Supplementary Card, expiration, termination or withdrawal from the Agreement,
§ 7.1. When executing a Payment Instruction submitted by a Customer/User, the Bank will ensure that the account of the Recipient's provider is credited with the amount of the Transaction not later than 1 Business Day after the Bank received the Payment Instruction. The above time limit may be extended by another Business Day in the case of a Transaction initiated by a paper order.	§ 7.1. When executing a Payment Instruction submitted by a Customer/Authorized User, the Bank will ensure that the account of the Recipient's provider is credited with the amount of the Transaction not later than 1 Business Day after the Bank received the Payment Instruction. The above time limit may be extended by another Business Day in the case of a Transaction initiated by a paper order.
§ 7.4. The Bank is entitled to refuse to execute a Payment Instruction submitted by a Customer/User if the Customer/User has failed to meet the conditions specified in the Agreement or the possibility or obligation to refuse results from separate laws and regulations. In the event of refusal to execute a Payment Instruction, the Bank, at a Branch, via the CitiPhone Telephone Banking Service, via Citibank Online, via the Recipient, or with the use of electronic communication means, will notify the Customer of such a refusal and, if possible, of the reasons behind such a refusal and of the procedure for rectifying the errors that have led to the refusal unless such a notification is not allowed under separate laws and regulations.	§ 7.4. The Bank is entitled to refuse to execute a Payment Instruction submitted by a Customer/Authorized User if the Customer/Authorized User has failed to meet the conditions specified in the Agreement or the possibility or obligation to refuse results from separate laws and regulations. In the event of refusal to execute a Payment Instruction, the Bank, at a Branch, via the CitiPhone Telephone Banking Service, via Citibank Online, via the Recipient, or with the use of electronic communication means, will notify the Customer of such a refusal and, if possible, of the reasons behind such a refusal and of the procedure for rectifying the errors that have led to the refusal unless such a notification is not allowed under separate laws and regulations.
§ 7.15. If the Transaction is initiated by or through a Recipient and the exact amount of the transaction is not known when the Customer/User consents to the Transaction, the Bank may effect a lock of funds on the payer's Card Account (also known as an 'authorization hold') only if the payer has agreed to have the relevant amount of funds locked. The Bank shall release the amount locked on the Card Account in accordance with the preceding sentences promptly after it has received the Payment Instruction and information about the specific amount of the payment transaction. § 7.16. The exchange rates applied by the Payment Organization for translating Citibank Credit Card Transactions into PLN and the associated translation rules are available on the Bank's website: https://www.citibank.pl/kursy-walut/. In the case of Transactions executed using a Card in currencies of the European Economic Area other than PLN, if the payment services providers of the payer and of the recipient are located in the European Economic Area, the Bank will send to the Customer or User, immediately after the receipt of the Payment Instruction by the Bank, an e-mail or text message with information on the total amount of currency translation fees expressed as a percentage margin in relation to the latest euro reference exchange rate published by the European Central Bank. The Bank will also send the information referred to in the preceding sentence to the Customer or User via Citibank Online or by e-mail once during the month in which the Bank received the payment instruction denominated in the currency referred to in the preceding sentence. § 7.17. Information on Transactions is available via Citibank Online, Citi Mobile, CitiPhone Telephone Banking Service and at Branches to: (a) the Customer – information on Transactions executed with the Primary Card and Supplementary Cards; (b) the User – information on Transactions executed with the Supplementary Card.	§ 7.15. If the Transaction is initiated by or through a Recipient and the exact amount of the transaction is not known when the Customer/Authorized User consents to such a Transaction, the Bank may effect a lock of funds on the payer's Card Account (also known as an 'authorization hold') only if the payer has agreed to have the relevant amount of funds locked. The Bank shall release the amount locked on the Card Account in accordance with the preceding sentences promptly after it has received the Payment Instruction and information about the specific amount of the payment transaction. § 7.16. The exchange rates applied by the Payment Organization for translating Citibank Credit Card Transactions into PLN and the associated translation rules are available on the Bank's website: https://www.citibank.pl/kursy-walut/. In the case of Transactions executed using a Card in currencies of the European Economic Area other than PLN, if the payment services providers of the payer and of the recipient are located in the European Economic Area, the Bank will send the Customer/Authorized User, immediately after the receipt of the Payment Instruction by the Bank, an e-mail or text message with information on the total amount of currency translation fees expressed as a percentage margin in relation to the latest euro reference exchange rate published by the European Central Bank. The Bank shall also send the information referred to in the preceding sentence to the Customer/Authorized User via Citibank Online or by e-mail once during the month in which the Bank received the payment instruction denominated in the currency referred to in the preceding sentence. § 7.17. Information on Transactions is available via Citibank Online, Citi Mobile, CitiPhone Telephone Banking Service and at Branches to: (a) the Customer – information on Transactions executed with the Primary Card and Supplementary Cards; (b) an Authorized User – information on Transactions executed with a Supplementary Card.
§ 7.26. By authorizing a BLIK Transaction, the Customer/User approves debiting the chosen BLIK Account with the amount of such a BLIK Transaction plus the fees and commissions as per the Table of	§ 7.26. By authorizing a BLIK Transaction, the Customer/Authorized User approves debiting the chosen BLIK Account with the amount of such a BLIK Transaction plus the fees and commissions as

Fees and Commissions. § 7.27. For security reasons, when executing Transactions using the PIN, triple entry of a wrong PIN will automatically block the PIN, which means that the Customer/User will not be able to make any PIN-based Transactions using the Card or Contactless Medium, as applicable, until its unblocking is agreed on with the Bank.	per the Table of Fees and Commissions. § 7.27. For security reasons, when executing Transactions using the PIN, triple entry of a wrong PIN will automatically block the PIN, which means that the Customer/Authorized User will not be able to make any PIN-based Transactions using the Card or Contactless Medium, as applicable, until its unblocking is agreed on with the Bank.
§ 7.34. The Bank does not allow the Customer/User to execute a Payment Instruction from the Card Account in the form of a SEPA Transfer Order, Transfer Order in Foreign Currency, Cross-border Transfer Order in PLN, Cross-border Transfer Order in EUR or a Cross-border Transfer Order in Foreign Currency.	§ 7.34. The Bank does not allow the Customer/Authorized User to execute a Payment Instruction from the Card Account in the form of a SEPA Transfer Order, Transfer Order in Foreign Currency, Cross-border Transfer Order in PLN, Cross-border Transfer Order in EUR or a Cross-border Transfer Order in Foreign Currency.
§ 7.36. The Bank will execute a Payment Instruction if the Credit Limit on the Card Account is sufficient to execute the Transaction, the Payment Instruction is not connected with any countries or entities covered by international sanctions or embargoes, in particular those imposed by the EU, US or UN and, additionally, with respect to an Internal Transfer Order in PLN or a Domestic Transfer Order in PLN from the Card Account, provided that: (a) the Customer/User has provided the Bank with or has confirmed to the Bank (including in the case of Pay by Link Transactions) the correct NRB of a valid Recipient's account, and in the case of a BLIK Phone-to-Phone Instant Transfer, the recipent's phone number registered in the BLIK Database, required to initiate or execute the Internal Transfer Order in PLN or the Domestic Transfer Order in PLN, and (b) the Customer/User has provided the Bank with or has confirmed to the Bank (in the case of Pay by Link Transactions) all information required to initiate or execute the Internal Transfer Order in PLN or the Domestic Transfer Order in PLN, i.e. the currency, amount of the Transaction, name of the Recipient and the transfer reference.	§ 7.36. The Bank will execute a Payment Instruction if the Credit Limit on the Card Account is sufficient to execute the Transaction, the Payment Instruction is not connected with any countries or entities covered by international sanctions or embargoes, in particular those imposed by the EU, US or UN and, additionally, with respect to an Internal Transfer Order in PLN or a Domestic Transfer Order in PLN from the Card Account, provided that: the Customer/Authorized User has provided the Bank with or has confirmed to the Bank (including in the case of Pay by Link Transactions) the correct NRB of a valid Recipient's account, and in the case of a BLIK Phone-to-Phone Instant Transfer, the recipent's phone number registered in the BLIK Database, required to initiate or execute the Internal Transfer Order in PLN or the Domestic Transfer Order in PLN, and (b) the Customer/Authorized User has provided the Bank with (or has confirmed to the Bank, in the case of Pay by Link Transactions) all information required to initiate or execute the Internal Transfer Order in PLN or the Domestic Transfer Order in PLN, i.e. the currency, amount of the Transaction, name of the Recipient and the transfer reference.
§ 7.38. The Bank will execute a Payment Instruction for Cash Deposit into the Card Account if the Customer/User has provided the Bank with the following: (a) for a Cash Deposit via an ATM: the PIN and the Cash Deposit amount; (b) for a Cash Deposit at a Branch: Card number/Card Account number in NRB format and the deposited amount.	§ 7.38. The Bank will execute a Payment Instruction for Cash Deposit into the Card Account if the Customer/Authorized User has provided the Bank with the following: (a) for a Cash Deposit via an ATM: the PIN and the Cash Deposit amount; (b) for a Cash Deposit at a Branch: Card number/Card Account number in NRB format and the deposited amount.
§ 7.42. After the lapse of the time limits set forth in Clauses 41–43 above, the Payment Instruction can be recalled or modified only upon agreement between the Customer/User and the relevant provider (Bank or Third Party Provider). For a payment transaction initiated by or through the Recipient, any recall or modification of a Payment Instruction after the lapse of the time limits set forth in this clause must also be approved by the Recipient.	§ 7.42. After the lapse of the time limits set forth in Clauses 39–41 above, the Payment Instruction can be recalled or modified only upon agreement between the Customer/Authorized User and the relevant provider (Bank or Third Party Provider). For a payment transaction initiated by or through the Recipient, any recall or modification of a Payment Instruction after the lapse of the time limits set forth in this clause must also be approved by the Recipient.
§ 7.46. Subject to Clauses 49 and 51–53 below, the Bank shall start executing a Payment Instruction upon receiving it unless the Bank and the Customer/User have agreed that the execution of the Payment Instruction will commence on another day, as specified in the Payment Instruction.	§ 7.46. Subject to Clauses 49 and 51–53 below, the Bank shall start executing a Payment Instruction upon receiving it unless the Bank and the Customer/Authorized User have agreed that the execution of the Payment Instruction will commence on another day, as specified in the Payment Instruction.
§ 7.49. In the case of Payment Instructions submitted by the Customer/User via the CitiPhone Telephone Banking Service, the Bank may confirm such a Payment Instruction by telephone on its submission day or on the next Business Day using the contact telephone number specified by the Customer/User – provided that the Customer/User was notified of such a requirement when they were submitting the Payment Instruction. In such case, the Payment Instruction will be deemed accepted for	§ 7.49. In the case of Payment Instructions submitted by the Customer/Authorized User via the CitiPhone Telephone Banking Service, the Bank may confirm such a Payment Instruction by telephone on its submission day or on the next Business Day using the contact telephone number specified by the Customer/Authorized User – provided that the Customer/Authorized User was notified of such a requirement when they were submitting the Payment Instruction. In such case,

execution after the above confirmation is received.	the Payment Instruction will be deemed accepted for execution after the above confirmation is received.
§ 7.51. If the execution of a Payment Instruction is conditional on the acceptance of an application or a complaint submitted by the Customer/User, the Payment Instruction will be deemed received on the day on which such application or complaint is granted.	§ 7.51. If the execution of a Payment Instruction is conditional on the acceptance of an application or a complaint submitted by the Customer/Authorized User, the Payment Instruction will be deemed received on the day on which such application or complaint is granted.
§ 8.7. The Customer shall control the amount of their Outstanding Balance to the Bank. Should the Credit Limit be overdrafted by the Customer/User, the Customer shall promptly repay the amount of the overdraft.	§ 8.7. The Customer shall control the amount of their Outstanding Balance to the Bank. Should the Credit Limit be overdrafted by the Customer/Authorized User, the Customer shall promptly repay the amount of the overdraft.
§ 13.13. Complaints may be filed as per the Agreement and these Terms and Conditions by: (a) the Customer – in respect of the Primary Card and Supplementary Cards; (b) the User – in respect of the Supplementary Card.	§ 13.13. Complaints may be filed as per the Agreement and these Terms and Conditions by: (a) the Customer – in respect of the Primary Card and Supplementary Cards; (b) The Authorized User – in respect of the Supplementary Card.
§ 14.1. The Customer/User shall exercise due diligence to protect the Card against loss or destruction and to protect the User Name and the Identification Code against disclosure.	§ 14.1. The Customer/Authorized User shall exercise due diligence to protect the Card against loss or destruction and to protect the User Name and the Identification Code against disclosure.
§ 16.1. The Bank informs the Customer that: (a) it will contact the Customer/User via telephone, SMS messages, MMS messages (in the case of marketing communications), e-mail messages or electronic messages available at Citibank Online, in particular with regard to matters related to the performance of the Agreement, in situations involving problems with execution of the Customer's/User's instructions, with security of the Customer's funds, or in the complaint handing process; (b) communication with the Customer via SMS messages, including under the CitiAlerts service, is effected in cooperation with a telecommunications company; (c) phone calls with the Bank are recorded by electronic means and may be used as evidence; (d) giving third parties access to the mobile phone or electronic mail, to which SMS messages or e-mail messages are sent may enable such parties to obtain information constituting banking secrecy or to make statements on behalf of, and on account of the Customer. § 16.2. The Customer/User undertakes to secure the access to the mobile phone or the electronic mail (e-mail) indicated to the Bank for communication purposes. The Primary Electronic Mail Address or Primary Mobile Phone Number registered with the Bank should be used solely by the Customer or User, as appropriate.	§ 16.1. The Bank informs the Customer that: (a) it will contact the Customer/Authorized User via telephone, SMS messages, MMS messages (in the case of marketing communications), e-mail messages or electronic messages available at Citibank Online, in particular with regard to matters related to the performance of the Agreement, in situations involving problems with execution of the Customer's/Authorized User's instructions, with security of the Customer's funds, or in the complaint handing process; (b) communication with the Customer via SMS messages, including under the CitiAlerts service, is effected in cooperation with a telecommunications company; (c) phone calls with the Bank are recorded by electronic means and may be used as evidence; (d) giving third parties access to the mobile phone or electronic mail, to which SMS messages or e-mail messages are sent may enable such parties to obtain information constituting banking secrecy or to make statements on behalf of, and on account of the Customer. § 16.2. The Customer/Authorized User undertakes to secure the access to the mobile phone or the electronic mail (e-mail) indicated to the Bank for communication purposes. The Primary Electronic Mail Address or Primary Mobile Phone Number registered with the Bank should be used solely by the Customer/Authorized User, as appropriate.
§ 16.4. The User and the Customer shall notify the Bank forthwith each time of any changes in the Personal Data of the User and the Primary Electronic Mail Address, Primary Mobile Phone Number and other phone numbers provided to the Bank.	§ 16.4. The Authorized User and the Customer shall notify the Bank forthwith each time of any changes in the Personal Data of the User and the Primary Electronic Mail Address, Primary Mobile Phone Number and other phone numbers provided to the Bank.
§ 17.1. The Bank provides Customers/Users with 24/7 access to Citibank Online and the CitiPhone Telephone Banking Service. The use of the CitiPhone Telephone Banking Service via a Consultant will be subject to a fee as per the valid Table of Fees and Commissions. Any tollable call to a Consultant shall activate the CitiPhone Telephone Banking Service, and thereby the charging of the fee for using the CitiPhone Telephone Banking Service by the Customer. If there are problems with Citibank Online and in the cases specified in the Terms and Conditions, the blocking of the credit card is free of charge and shall not activate the fee for using the CitiPhone Telephone Banking Service. § 17.2. The Customer may opt out of and reactivate the CitiPhone Telephone Banking Service at all	§ 17.1. The Bank provides Customers/Authorized Users with 24/7 access to Citibank Online and the CitiPhone Telephone Banking Service. The use of the CitiPhone Telephone Banking Service via a Consultant will be subject to a fee as per the valid Table of Fees and Commissions. Any tollable call to a Consultant shall activate the CitiPhone Telephone Banking Service, and thereby the charging of the fee for using the CitiPhone Telephone Banking Service by the Customer. If there are problems with Citibank Online and in the cases specified in the Terms and Conditions, the blocking of the Card shall be free of charge and shall not activate the fee for using the CitiPhone Telephone Banking Service.

times. § 17.3. In order to be able to use the CitiPhone Telephone Banking Service, the Customer/User must have a touch-tone telephone set and establish connection with the relevant number specified by the Bank. § 17.4. The Customer/User shall create and change their CitiPhone PIN via CitiPhone. The information concerning the assignment and each change of CitiPhone PIN will be sent to the Customer in the form of SMS messages to their Primary Mobile Phone Number and by email to the Primary Electronic Mail Address. § 17.5. The Bank provides Customers/Users with 24/7 access to Citibank Online. Citibank Online will be activated upon issuance of the Payment Card (Card). Any references in these Terms and Conditions to Citibank Online refer to Citi Mobile, unless otherwise stated. § 17.6. By means of the CitiPhone Telephone Banking Service, Citibank Online, the Customer/User may in particular: (a) obtain information about the Card Account balance and operations; (b) execute Transactions; (c) transfer Transactions to the 'Comfort' Installment Payment Plan (solely the Customer); (d) issue other instructions accepted by the Bank.	§ 17.2. The Customer may opt out of and reactivate the CitiPhone Telephone Banking Service at all times. § 17.3. In order to be able to use the CitiPhone Telephone Banking Service, the Customer/Authorized User must have a touch-tone telephone set and establish connection with the relevant number specified by the Bank. § 17.4. The Customer/Authorized User assigns and changes their CitiPhone PIN via CitiPhone. The information concerning the assignment and each change of CitiPhone PIN will be sent to the Customer in the form of SMS messages to their Primary Mobile Phone Number and by email to the Primary Electronic Mail Address. § 17.5. The Bank provides Customers/Authorized Users with 24/7 access to Citibank Online. Citibank Online will be activated upon issuance of the Payment Card (Card). Any references in these Terms and Conditions to Citibank Online refer to Citi Mobile, unless otherwise stated. § 17.6. By means of the CitiPhone Telephone Banking Service, Citibank Online, the Customer/Authorized User may in particular: (a) obtain information about the Card Account balance and operations; (b) execute Transactions; (c) transfer Transactions to the 'Comfort' Installment Payment Plan (solely the Customer); (d) issue other instructions accepted by the Bank.
§ 17.8. The Customer/User may not communicate illegal content using the Citibank Online or the CitiPhone Telephone Banking Service or use these services in a manner contrary to their social and economic purpose or principles of community life.	§ 17.8. The Customer/Authorized User may not communicate illegal content using the Citibank Online or the CitiPhone Telephone Banking Service or use these services in a manner contrary to their social and economic purpose or principles of community life.
§ 17.13. The manner of operation and the use of Citibank Online is described in the relevant user manuals available on the Bank's websites. The manuals referred to in the preceding sentence provide for the specific rules on electronic identification of the Customer/User and on how the Customer/User is to act when using access to the Card Account via Citibank Online. § 17.14. The Customer and the User is obliged to keep confidential all information the disclosure of which may compromise the safeguards of the operations ordered via the CitiPhone Telephone Banking Service and Citibank Online, in particular the Identification Code. § 17.15. If the Customer/User discloses the information referred to in Clause 14 above to third parties and if such third parties execute any operations via Citibank Online, the said operations will be charged solely to the Customer, subject to § 14 above. § 17.16. The Customer undertakes to use CitiPhone Telephone Banking Service and Citibank Online in accordance with applicable laws, including these Terms and Conditions. Any use of CitiPhone and Citibank Online in breach of law may serve as the basis for termination of the Agreement, in accordance with § 24.2. below. For security reasons, the Bank reserves the right to terminate the connection with the Customer after the lapse of a period specified by the Bank following the Customer's last activity. The maximum Customer session idle timeout is five minutes. The Customer can connect again to Citibank Online or Citi Mobile after re-authentication or Strong Authentication. § 17.17. The Bank affirms that it will provide the Customer/User with computer programs and files necessary for the purpose of using Citibank Online.	§ 17.14. The manner of operation and the use of Citibank Online is described in the relevant user manuals available on the Bank's websites. The manuals referred to in the preceding sentence provide for the specific rules on electronic identification of the Customer/Authorized User and on how the Customer/Authorized User is to act when using access to the Card Account via Citibank Online. § 17.15. The Customer and Authorized User is obliged to keep confidential all information the disclosure of which may compromise the safeguards of the operations ordered via the CitiPhone Telephone Banking Service and Citibank Online, in particular the Identification Code. § 17.16. If the Customer/Authorized User discloses the information referred to in Clause 15 above to third parties and if such third parties execute any operations via Citibank Online, the said operations will be charged solely to the Customer, subject to § 14 above. § 17.17. The Customer/Authorized User undertakes to use CitiPhone Telephone Banking Service and Citibank Online in accordance with applicable laws, including these Terms and Conditions. Any use of CitiPhone and Citibank Online in breach of law may serve as the basis for termination of the Agreement, in accordance with § 24.2. below. For security reasons, the Bank reserves the right to terminate the connection with the Customer/Authorized User after the lapse of a period specified by the Bank following the Customer's last activity. The maximum Customer session idle timeout is five minutes. The Customer/Authorized User can reconnect to Citibank Online or Citi Mobile after repeated Authentication or Strong Authentication. § 17.18. The Bank affirms that it will provide the Customer/Authorized User with computer programs and files necessary for the purpose of using Citibank Online.

§ 18.1. The cookies used by the Bank do not store personal data that enable the identification of an online service user. They are used, among other things, to remember the Users' preferences, protect websites or conduct marketing campaigns. Unless the User accepts cookies, some functionalities on the Bank's websites will not be available. 2. The following types of Cookies are used by the Bank's online services: (a) persistent cookies – they are recorded on the device used by the End User, even after leaving the website. They store and remember information about the User's preferences, e.g. the user name (login) when the transaction service system is logged in to. This means that this field will be pre-filled each time the service is accessed. By accepting this type of cookies the User agrees to store information on the User's device. (i) In order to remove a Citibank Online and Bank website user name, select the existing name and choose the "Delete user" option from the menu. (ii) In order to remove a Citi Mobile user name, select the existing name, choose the "Edit" option from the menu and tap the "recycle bin" icon. (b) session cookies – they are necessary to maintain exchange of information between the Bank's server and the web browser, and ensure that Citibank Online, Bank's website, and Citi Mobile contents are displayed correctly and that the functionalities of these services can be used. The Bank stores and accesses this information to identify a given session (dialogue between the browser and the server) and End Users (communicating with the server at the same time). (c) third party cookies – they allow third parties to analyze information about the number of visits and users' website behavior. However, they are not Personal Data allowing the User to be identified as a Bank Customer. The purpose of collecting and processing such cookies is to gather information about the profile of the Bank's website visitors, their behaviors, preferences and interest in individual products. The companies that provide analytical services for the Bank include Gemius, Google and others. Such cookies are not used in Citibank Online and Citi Mobile services.	§ 18.1. The cookies used by the Bank do not store personal data that enable the identification of an online service user. They are used, among other things, to remember the Users' preferences, protect websites or conduct marketing campaigns. Unless the User accepts cookies, some functionalities on the Bank's websites will not be available. § 18.2. The following types of Cookies are used by the Bank's online services: (a) persistent cookies – they are saved on the device used by the End User, even after the website is left. They store and remember information about the User's preferences, e.g. the user name (login) when the transaction service system is logged in to. This means that this field will be pre-filled each time the service is accessed. By accepting this type of cookies the User agrees to store information on the User's device. (i) In order to remove a Citibank Online and Bank website user name, select the existing name and choose the "Delete user" option from the menu. (ii) In order to remove a Citi Mobile user name, select the existing name, choose the "Edit" option from the menu and tap the "recycle bin" icon. (b) session cookies – they are necessary to maintain exchange of information between the Bank's server and the web browser, and ensure that Citibank Online, Bank's website, and Citi Mobile contents are displayed correctly and that the functionalities of these services can be used. The Bank stores and accesses this information to identify a given session (dialogue between the browser and the server) and End Users (communicating with the server at the same time). (c) third party cookies – they allow third parties to analyze information about the number of visits and users' website behavior. However, they are not Personal Data allowing the User to be identified as a Bank Customer. The purpose of collecting and processing such cookies is to gather information about the profile of the Bank's website visitors, their behaviors, preferences and interest in individual products. The companies that provide analytical services for the Bank include Gemius, Google and others. Such cookies are not used in Citibank Online and Citi Mobile services.
§ 19.1. The Bank enables Customers/Users to make BLIK Transactions in Citi Mobile.	§ 19.1. The Bank enables Customers/Authorized Users to make BLIK Transactions in Citi Mobile.
§ 19.4. A BLIK Payment may be made provided that BLIK Payments are supported by the point-of-sale (POS) terminal or by the Online Payments Operator selected by the Customer/User. A BLIK Cash Withdrawal may be made provided that BLIK Cash Withdrawal is supported by the ATM. A BLIK Phone-to-Phone Instant Transfer may be made provided that the recipient uses the BLIK Phone-to-Phone Instant Transfer service. § 19.5. The BLIK Code is generated in Citi Mobile. The BLIK Code is valid for 120 seconds from its generation. Only one valid BLIK Code may exist for a given Customer/User at any time. A BLIK Code expires upon the lapse of the BLIK Code validity time or upon the Authorization of the BLIK Transaction for which the BLIK Code has been generated. When a BLIK Code has expired, the Customer can generate a new Code. Generating a BLIK Code requires enabling the Citi Mobile Token service.	§ 19.4. A BLIK Payment may be made provided that BLIK Payments are supported by the point-of-sale (POS) terminal or by the Online Payments Operator selected by the Customer/Authorized User. A BLIK Cash Withdrawal may be made provided that BLIK Cash Withdrawal is supported by the ATM. A BLIK Phone-to-Phone Instant Transfer may be made provided that the recipient uses the BLIK Phone-to-Phone Instant Transfer service. § 19.5. The BLIK Code is generated in Citi Mobile. The BLIK Code is valid for 120 seconds from its generation. Only one valid BLIK Code may exist for a given Customer/Authorized User at any time. A BLIK Code expires upon the lapse of the BLIK Code validity time or upon the correct Authentication of the BLIK Transaction for which the BLIK Code has been generated. When a BLIK Code has expired, the Customer can generate a new Code. Generating a BLIK Code requires enabling the Citi Mobile Token service.
§ 20.1. Prior to making the first BLIK Phone-to-Phone Instant Transfer, the Customer/User must agree for Citi Mobile to access the address book on the Mobile Device. If the Customer does not consent for Citi Mobile to access the address book, the Customer will need to enter the mobile phone number of	§ 20.1. Prior to making the first BLIK Phone-to-Phone Instant Transfer, the Customer/Authorized User must agree for Citi Mobile to access the address book on the Mobile Device. If the Customer does not consent for Citi Mobile to access the address book, the Customer will need to enter the

the BLIK Phone-to-Phone Instant Transfer recipient on their own. § 20.2. In order to make a BLIK Phone-to-Phone Instant Transfer, it is necessary for the Customer/User to log in to Citi Mobile, provide the Recipient's cell phone number, the amount of Domestic Transfer Order in PLN or of Internal Transfer Order in PLN, and the recipient's full name. A BLIK Phone-to-Phone Instant Transfer is available provided that the Recipient's bank account is linked in the BLIK System with the Recipient's mobile phone number entered by the Customer/User.	mobile phone number of the BLIK Phone-to-Phone Instant Transfer recipient on their own. § 20.2. In order to make a BLIK Phone-to-Phone Instant Transfer, it is necessary for the Customer/Authorized User to log in to Citi Mobile and provide the Recipient's cell phone number, the amount of Domestic Transfer Order in PLN or of Internal Transfer Order in PLN, and the recipient's full name. A BLIK Phone-to-Phone Instant Transfer is available provided that the Recipient's bank account is linked in the BLIK System with the Recipient's mobile phone number entered by the Customer/Authorized User.
§ 20.5. If a BLIK Phone-to-Phone Instant Transfer is denied, the Bank notifies the Customer/User of the denial via Citi Mobile or by sending a text message to the Primary Mobile Phone Number. § 20.6. The Customer may register their Card Account as the target account for BLIK Phone-to-Phone Instant Transfers ordered by third parties. For this purpose, it is necessary for the Customer/User to register via Citi Mobile in the BLIK Database and indicate the Card Account for receipt of funds. § 20.7. The Customer/User may disable the functionality of receiving BLIK Phone-to-Phone Instant Transfers or change the designated account. For this purpose, the Customer/User should submit a request for deregistration from the BLIK Database in Citi Mobile. Receiving BLIK Phone-to-Phone Instant Transfers again requires re-registration with the BLIK Database.	§ 20.5. If a BLIK Phone-to-Phone Instant Transfer is denied, the Bank notifies the Customer/Authorized User of the denial via Citi Mobile or by sending a text message to the Primary Mobile Phone Number. § 20.6. The Customer may register their Card Account as the target account for BLIK Phone-to-Phone Instant Transfers ordered by third parties. For this purpose, it is necessary for the Customer/Authorized User to register via Citi Mobile in the BLIK Database and indicate the Card Account for receipt of funds. § 20.7. The Customer/Authorized User may disable the functionality of receiving BLIK Phone-to-Phone Instant Transfers or change the designated account. For this purpose, the Customer/Authorized User should submit a request for deregistration from the BLIK Database in Citi Mobile. Receiving BLIK Phone-to-Phone Instant Transfers again requires re-registration with the BLIK Database.
§ 23.22. A User will not be authorized to issue any instructions relating to the Plan.	§ 23.22. An Authorized User will not be authorized to issue any instructions relating to the Plan.
§ 27.1. If a Payment Instruction is submitted directly by the Customer/User, the Bank, unless it proves that the account of the Payment Services Provider of the Recipient was credited within the time limits specified in § 7.1. of the Terms and Conditions, will be liable toward the Customer for non-performance or undue performance of the Transaction unless: (a) the Customer fails to notify the Bank, promptly, but in any case not later than in 13 months from the date on which the payment account was debited, of the unauthorized, non-performed or unduly performed Transactions, using the procedure specified in the Terms and Conditions; (b) such non-execution or undue execution of the Transaction is caused by an event of force majeure or results from other laws or regulations; (c) the account of the Recipient is credited in accordance with the Unique Identifier provided to the Bank by the Customer/User. § 27.2. If the Bank is liable under Clause 1 above, it will promptly restore the debited Card Account to the status that would have existed if the non-performance or undue performance of the Transaction had not occurred. The value date of crediting the payment account of the Customer may not be later than the value date of debiting such an amount. § 27.3. If the Payment Instruction is submitted by the Customer/User to a Third Party Provider, the Bank will reimburse the Customer for the amount of the non-executed or unduly executed payment transaction or, if necessary, it will restore the debited Card Account to the balance that would have existed if such undue execution had not occurred.	§ 27.1. If a Payment Instruction is submitted directly by the Customer/Authorized User, the Bank, unless it proves that the account of the Payment Services Provider of the Recipient was credited within the time limits specified in § 7.1. of the Terms and Conditions, will be liable toward the Customer for non-performance or undue performance of the Transaction unless: (a) the Customer fails to notify the Bank, promptly, but in any case not later than in 13 months from the date on which the payment account was debited, of the unauthorized, non-performed or unduly performed Transactions, using the procedure specified in the Terms and Conditions; (b) such non-execution or undue execution of the Transaction is caused by an event of force majeure or results from other laws or regulations; (c) the account of the Recipient is credited in accordance with the Unique Identifier provided to the Bank by the Customer/Authorized User. § 27.2. If the Bank is liable under Clause 1 above, it will promptly restore the debited Card Account to the status that would have existed if the non-performance or undue performance of the Transaction had not occurred. The value date of crediting the payment account of the Customer may not be later than the value date of debiting such an amount. § 27.3. If the Payment Instruction is submitted by the Customer/Authorized User to a Third Party Provider, the Bank will reimburse the Customer for the amount of the non-executed or unduly executed payment transaction or, if necessary, it will restore the debited Card Account to the balance that would have existed if such undue execution had not occurred.
§ 1.7. In the case of non-executed or unduly executed Transaction for which the Bank, as the provider of the Recipient, is not liable under Clauses 5 and 6 above, the liability to the Payer (other than the	§ 27.7. In the case of non-executed or unduly executed Transaction for which the Bank, as the provider of the Recipient, is not liable under Clauses 5 and 6 above, the liability to the Payer (other

Customer) will be borne by the service provider of that Payer. In such a case the service provider of the Payer (other than the Customer) will promptly reimburse that Payer for the amount of the non-executed or unduly executed payment transaction or, where the Payer uses a payment account, it will restore the charged payment account to the balance that would have existed if non-execution or improper execution of the payment transaction had not occurred. The obligation referred to in the previous sentence is not applicable to the service provider of the Payer (other than the Customer) if it proves that the Bank, as the provider of the Recipient, received the amount of the payment transaction, even if the payment transaction was executed with a delay. In such a case the Bank, as the provider of the Recipient, will credit the Card Account with the amount at the value date no later than the value date at which the Card Account would have been credited if the payment transaction had been executed correctly. If a Transaction initiated by the Customer/User or initiated by or through the Recipient is not executed or is unduly executed, excluding any Transaction initiated by the Customer/User, for which the Unique Identifier provided by the Customer was incorrect, the Bank, irrespective of any liability under the above provisions, will promptly initiate any steps, on request of the Customer, to track the Transaction and will notify the Customer of the results of such tracking, such steps being free of charge for the Customer. In the case of a Transaction in which the Unique Identifier provided by the Customer was incorrect, the Bank will promptly initiate any steps to recover the amount of the Transaction made with the use of such incorrect Unique Identifier, in particular on the terms and in the manner set forth in the Payment Services Act. If funds are recovered, the Bank will charge a fee to the Customer as per the Table of Fees and Commissions.	than the Customer) will be borne by the service provider of that Payer. In such a case the service provider of the Payer (other than the Customer) will promptly reimburse that Payer for the amount of the non-executed or unduly executed payment transaction or, where the Payer uses a payment account, it will restore the charged payment account to the balance that would have existed if non-execution or improper execution of the payment transaction had not occurred. The obligation referred to in the previous sentence is not applicable to the service provider of the Payer (other than the Customer) if it proves that the Bank, as the provider of the Recipient, received the amount of the payment transaction, even if the payment transaction was executed with a delay. In such a case the Bank, as the provider of the Recipient, will credit the Card Account with the amount at the value date no later than the value date at which the Card Account would have been credited if the payment transaction had been executed correctly. § 27.8. If a Transaction initiated by the Customer/Authorized User or initiated by or through the Recipient is not executed or is unduly executed, excluding any Transaction initiated by the Customer/Authorized User, for which the Unique Identifier provided by the Customer was incorrect, the Bank, irrespective of any liability under the above provisions, will promptly initiate any steps, on request of the Customer, to track the Transaction and will notify the Customer of the results of such tracking, such steps being free of charge for the Customer. In the case of a Transaction in which the Unique Identifier provided by the Customer was incorrect, the Bank will promptly initiate any steps to recover the amount of the Transaction made with the use of such incorrect Unique Identifier, in particular on the terms and in the manner set forth in the Payment Services Act. If funds are recovered, the Bank will charge a fee to the Customer as per the Table of Fees and Commissions.
§ 27.10. The Customer will not be entitled to a refund of the amount of an authorized Transaction initiated by the Recipient if: (a) the Customer/User gave their consent to execute the Transaction directly to the Bank, and (b) information on the future Transaction was given to the Customer by the Bank or the Recipient, in an agreed manner, at least 4 weeks before the date of execution of the order or was made available to the Customer by the Bank or the Recipient, in an agreed manner, for the period of at least 4 weeks before the date of execution of the order.	§ 27.11. The Customer will not be entitled to a refund of the amount of an authorized Transaction initiated by the Recipient if: (a) the Customer/Authorized User gave their consent to execute the Transaction directly to the Bank, and (b) information on the future Transaction was given to the Customer by the Bank or the Recipient, in an agreed manner, at least 4 weeks before the date of execution of the order or was made available to the Customer by the Bank or the Recipient, in an agreed manner, for the period of at least 4 weeks before the date of execution of the order.
Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.	
Factual background behind the amendment: Revision of the wording further to the change of the defined term from User to Authorized User and adding clarity to the wording by including also an Authorized User	
Pre-amendment wording	**Post-amendment wording**

§ 17.22. The Customer should not open or reply to e-mails in which they are asked to provide personal data or Identification Codes. Such cases should be reported to the Bank. § 17.23. The Customer should not open suspicious links or attachments of unknown origin received in e-mail, SMS, MMS, and push messages.	§ 17.23. The Customer/Authorized User should not open or reply to e-mails in which they are asked to provide personal data or Identification Codes. Such cases should be reported to the Bank. § 17.24. The Customer/Authorized User should not open suspicious links or attachments of unknown origin received in e-mail, SMS, MMS, and push messages.
§ 17.25. When logging in to Citibank Online or Citi Mobile, the Customer will not be asked by the Bank to provide the telephone type, telephone number and will not be requested to install software or certificate on their phones or other devices.	§ 17.26. When logging in to Citibank Online or Citi Mobile, the Customer/Authorized User will not be asked by the Bank to provide the telephone type, telephone number and will not be requested to install software or certificate on their phones or other devices.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Clarification of the provisions regarding authentication for authorization purposes	
Pre-amendment wording	**Post-amendment wording**
§ 7.20. Save for Transactions made in the manner specified in § 7.23.-§ 7.25, § 7.30.-§ 7.33 and § 7.45 below, or a Transaction made as result of concluding an Understanding, as described in § 23.9 below, a Transaction made with a Card shall be deemed authorized by the Customer/User if it has been confirmed by using the PIN, a Mobile Device Unlocking Method or a Biometric Method or affixing the signature of the Customer/User on the debit document in accordance with the signature affixed on the Card or the Specimen Signature – where no Strong Authentication is required. By authorizing a Transaction, the Customer/User approves debiting the Card Account with the amount of the Transaction plus the fees and commissions as per the Table of Fees and Commissions. § 7.21. An Instruction for Cash Deposit into the Card Account: (a) in the case of a cash deposit made via an ATM – will be deemed authorized if it is confirmed by the PIN; (b) at a Branch – will be deemed authorized if it is confirmed by the PIN or signature of the Customer. § 7.22. A Cash Withdrawal from an ATM by means of a Card shall be deemed authorized if it is confirmed by the PIN, a Mobile Device Unlocking Method or by a Biometric Method. A Cash Withdrawal made from ATMs in Poland or abroad by means of a Card is subject to restrictions provided for by applicable laws. § 7.23. A BLIK Cash Withdrawal Instruction is considered authorized by the Customer/User, if the Customer/User has authorized its execution by logging into Citi Mobile, generating a BLIK Code, entering the generated BLIK Code at the ATM, and confirming the Payment Instruction in Citi Mobile by selecting the appropriate function button used to deliver the Payment Instruction to the Bank and performing Mobile Authentication – if the Bank requires Strong Authentication. § 7.24. A BLIK Phone-to-Phone Instant Transfer Instruction is deemed authorized by the Customer/User if the Customer/User has given his/her consent to its execution by logging into Citi Mobile and confirming the Payment Instruction in Citi Mobile by selecting the appropriate function button used to	§ 7.20. Save for Transactions made in the manner specified in § 7.23.-§ 7.25, § 7.30.-§ 7.33 and § 7.45 below, or a Transaction made as result of concluding an Understanding, as described in § 23.9 below, if a Transaction is made with a Card, the Authentication for Authorization purposes shall be effected through the presentation of the Card and PIN confirmation, or through the presentation of a Virtual Card and confirmation by means of a Mobile Device Unlocking Method or a Biometric Method, or upon the signature by the Customer/Authorized User of the debit document in accordance with the signature affixed on the Card or the Specimen Signature – where no Strong Authentication is required. The Customer/Authorized User shall Authenticate a Transaction in order to consent to debiting the Card Account with the amount of the Transaction plus the fees and commissions as per the Table of Fees and Commissions. § 7.21. In the case of an Instruction for Cash Deposit into the Card Account, Authentication for Authorization purposes shall be effected through: (a) the presentation of the Card and confirmation with the PIN – if cash is deposited via an ATM, (b) confirmation with the Customer's PIN or signature – if cash is deposited at a Branch. § 7.22. If a Cash Withdrawal from an ATM is made with a Card, the Authentication for the purpose of Authorizing it shall be effected through the presentation of the Card and confirmation with the PIN or through a Mobile Device Unlocking Method or a Biometric Method. A Cash Withdrawal made from ATMs in Poland or abroad by means of a Card is subject to restrictions provided for by applicable laws. § 7.23. In the case of an Instruction for BLIK Cash Withdrawal, Authentication for Authorization purposes shall be effected by the Customer/Authorized User by logging in to Citi Mobile, generating a BLIK Code, entering the generated BLIK Code at the ATM, and confirming the Payment Order in Citi Mobile by selecting the appropriate function button used to deliver the Payment Instruction to the Bank, as well as by performing a Mobile Authentication – if the Bank requires

deliver the Payment Instruction to the Bank and performing Mobile Authentication – if the Bank requires Strong Authentication. § 7.25. A BLIK Payment Instruction shall be deemed authorized by the Customer/User if the Customer/User has authorized its execution by logging into Citi Mobile, generating a BLIK Code, entering the generated BLIK Code at a point-of-sale (POS) terminal or through an Online Payments Operator selected by the Customer/User, confirming the Payment Instruction in Citi Mobile by selecting the appropriate function button used to deliver the Payment Instruction to the Bank, and performing Mobile Authentication – if the Bank requires Strong Authentication.	Strong Authentication. § 7.24. In the case of a Payment Instruction for BLIK Phone-to-Phone Instant Transfer, Authentication for Authorization purposes shall be effected by way of logging in to Citi Mobile and confirming the Payment Instruction in Citi Mobile by selecting the appropriate function button used to deliver the Payment Instruction to the Bank and by completing a Mobile Authentication – if the Bank requires Strong Authentication. § 7.25. In the case of a BLIK Payment Transaction Instruction, Authentication for Authorization purposes shall be effected by logging in to Citi Mobile, generating a BLIK Code, entering the generated BLIK Code in the point of sale (POS) terminal or via the Online Payments Operator selected by the Customer/Authorized User, confirmation of the Payment Instruction in Citi Mobile by selecting the appropriate function button used to deliver the Payment Instruction to the Bank and completing a Mobile Authentication – if the Bank requires Strong Authentication.
§ 7.30. In the case of a Contactless Transaction: (a) equal to or above the Contactless Transaction Value Limit, or in the cases stipulated in § 7.64. below, the Transaction shall be deemed authorized if it has been confirmed by entering the PIN, by a Mobile Device Unlocking Method or by a Biometric Method. Besides, where Strong Authentication is not required by the Bank, the Transaction shall be deemed authorized if confirmed with the Customer's/User's signature on the debit document matching the signature on the Card; (b) below the Contactless Transaction Value Limit – the Transaction shall be deemed authorized upon the transmission of the Card or Contactless Medium details saved in the Contactless Module, as such details are required to execute the Transaction, by putting the Card or Contactless Medium in the proximity of a device capable of reading the details stored in the Contactless Module. In the cases set forth in § 7.64. below, the Transaction shall be deemed authorized upon the confirmation with the PIN, by a Mobile Device Unlocking Method or by a Biometric Method; (c) in the case of Contactless Transactions other than specified in (a) and (b) above, where the Bank is not obligated to apply Strong Authentication under applicable provisions of law, the Transaction shall be deemed authorized upon the transmission of the Card or Contactless Medium details saved in the Contactless Module, as such details are required to execute the Transaction, by putting the Card or Contactless Medium in the proximity of a device capable of reading the details stored in the Contactless Module. § 7.31. In the case of a device where transactions are initiated through the confirmation of being the Card holder, the Transaction shall be authorized by the physical presentation of the Card by the Customer/User in the device and PIN confirmation. In cases where Strong Authentication is not required under applicable laws, the Transaction shall be authorized through physical presentation of the Card in the device. § 7.32. In the case of Transactions executed remotely without physical presentation of the Card (executed over the phone, in writing or via the Internet), the Transaction shall be deemed authorized by the Customer/User upon the provision by the latter of the Card or Customer/User details, depending on the Recipient's requirements, including the name and surname, the Identification Code, the number and expiry date of the Card or CVV2/CVC2 code, and confirmation of the Transaction (if required by the Bank) with the 3D Secure Authentication or a Mobile Authentication or Citibank Online Authentication or by a Mobile Device Unlocking Method or a Biometric Method.	§ 7.30. In the case of a Contactless Transaction: (a) equal to or above the Contactless Transaction Value Limit or in the cases specified in § 7.62. below, the Authentication for Authorization purposes shall be effected by presenting the Card and PIN confirmation or by presenting the Virtual Card and confirmation with a Mobile Device Unlocking Method or a Biometric Method. Furthermore, in cases where the Bank does not require Strong Authentication, Authentication for Authorization purposes shall be effected by the Customer/Authorized User affixing a signature on the debit document matching the signature on the Card; (b) below the Contactless Transaction Value Limit – Authentication for Authorization purposes shall be deemed effected upon the transmission of the Card or Contactless Medium details stored in the Contactless Module, as such details are required to execute the Transaction, by putting the Card or Contactless Medium in the proximity of a device capable of reading the details stored in the Contactless Module. In the cases specified in § 7.62. below, Authentication for Authorization purposes shall be effected by presenting the Card and PIN confirmation or by presenting the Virtual Card and confirmation with a Mobile Device Unlocking Method or a Biometric Method. (c) Authentication for Authorization purposes shall be effected upon the transmission of the Card or Contactless Medium details stored in the Proximity Module, as such details are required to execute the Transaction, by tapping the Card or Contactless Medium to a device capable of reading the details stored in the Proximity Module – this applies to Contactless Transactions other than those specified in points (a) and (b) above, where the Bank is not obliged to use Strong Authentication under applicable law. § 7.31. In the case of a device where transactions are initiated through the confirmation of being the Card holder, Authentication for Authorization Purposes shall be effected by the physical presentation of the Card by the Customer/Authorized User in the device and PIN confirmation. In cases where Strong Authentication is not required under applicable laws, Authentication for Authorization Purposes shall be effected through physical presentation of the Card in the device. § 7.32. In the case of Transactions made remotely without physical presentation of the Card (over the phone, in writing or via the Internet), Authentication for Authorization purposes shall be effected by the provision of the Card or Customer/Authorized User details, depending on the

§ 7.33. The use of the Card number and the CitiPhone PIN, or of the CitiPhone PIN only where the Customer/User has enabled the Incoming Call Identification Service for placing telephone Payment Instructions constitutes the Customer's/User's consent for the execution of such Payment Instructions by the Bank, inclusive of the debiting of the Card Account.	Recipient's requirements, including the name and surname, the Identification Code, the number and expiry date of the Card or CVV2/CVC2 code, and confirmation of the Transaction (if required by the Bank) with the 3D Secure Authentication or a Mobile Authentication or Citibank Online Authentication or by a Mobile Device Unlocking Method or a Biometric Method. § 7.33. The use of the Card number and CitiPhone PIN, or of the CitiPhone PIN only where the Customer/Authorized User has enabled the Incoming Call Identification service for placing telephone Payment Instructions constitutes the Authentication of such Payment Instructions by the Customer/Authorized User for the purpose of Transaction Authorization.
§ 7.40. Subject to Clauses 43 and 44 below, Payment Instructions authorized by the Customer/User and delivered to the Bank will be deemed to be confirmed by the Customer/User and instructed to the Bank for execution in a valid and effective manner. The Customer/User may not cancel or modify any Payment Instruction after it is received by the Bank.	§ 7.40. Subject to Clauses 43 and 44 below, Payment Instructions Authenticated by the Customer/Authorized User and delivered to the Bank shall be deemed confirmed by the Customer/User and made to the Bank for execution in a valid and effective manner. The Customer/Authorized User may not cancel or modify any Payment Instruction after it has been received by the Bank.
§ 7.47. If a Payment Instruction is received by the Bank on a day that is not a Business Day for the Bank or on a Business Day, but after the cut-off time specified by the Bank in the Cut-off Times List, the Payment Instruction is deemed to have been received by the Bank on the first Business Day following that day, except that BLIK Phone-to-Phone Instant Transfers shall be executed immediately and the crediting of the Recipient's account with the transferred amount shall be effected upon the submission of a Payment Instruction for such transfer. Where the Authorization concerns subsequent payment transactions, the withdrawal shall apply to all payment transactions that have not been executed, unless the Customer indicated otherwise.	§ 7.47. If a Payment Instruction is received by the Bank on a day that is not a Business Day for the Bank or on a Business Day, but after the cut-off time specified by the Bank in the Cut-off Times List, the Payment Instruction is deemed to have been received by the Bank on the first Business Day following that day, except that BLIK Phone-to-Phone Instant Transfers shall be executed immediately and the crediting of the Recipient's account with the transferred amount shall be effected upon the submission of a Payment Instruction for such transfer. Where the Authorization concerns subsequent payment transactions, the withdrawal shall apply to all payment transactions that have not been executed, unless the Customer indicated otherwise.
§ 19.5. The BLIK Code is generated in Citi Mobile. The BLIK Code is valid for 120 seconds from its generation. Only one valid BLIK Code may exist for a given Customer/User at any time. A BLIK Code expires upon the lapse of the BLIK Code validity time or upon the Authorization of the BLIK Transaction for which the BLIK Code has been generated. When a BLIK Code has expired, the Customer can generate a new Code. Generating a BLIK Code requires enabling the Citi Mobile Token service.	§ 19.5. The BLIK Code is generated in Citi Mobile. The BLIK Code is valid for 120 seconds from its generation. Only one valid BLIK Code may exist for a given Customer/Authorized User at any time. A BLIK Code expires upon the lapse of the BLIK Code validity time or upon the correct Authentication of the BLIK Transaction for which the BLIK Code has been generated. When a BLIK Code has expired, the Customer can generate a new Code. Generating a BLIK Code requires enabling the Citi Mobile Token service.
§ 7.43. A Payment Instruction submitted via: (a) Citibank Online (including a Payment Instruction for a Pay by Link Transaction) or Citi Mobile will be deemed authorized by the Customer/User if the Customer/User has given their consent to execute it by way of logging in to Citibank Online or Citi Mobile, entering (or confirming – in the case of Pay by Link Transactions) the details of the Payment Instruction and confirming the execution of the Payment Instruction by selecting the relevant function button used to submit the Payment Instruction to the Bank and by entering the relevant Authorization Code or performing a Mobile Authentication (including based on an Authorization Code) – if the Bank requires strong authentication, (b) the CitiPhone Telephone Banking Service will be deemed authorized by the Customer/User if the Customer/User has given their consent to execute it, after having entered the Card number and having confirmed it with the CitiPhone PIN, or after having it confirmed only with the CitiPhone PIN in a situation where the Customer has activated the Incoming Call Identification Service, (c) a Branch will be deemed authorized by the Customer/User after the identity of the Customer/User is verified against the document that confirms their identity, or by entering PIN, and, then, by confirming the Payment Instruction with a signature or PIN.	§ 7.43. In the case of a Payment Instruction placed via: a) Citibank Online (including a Payment Instruction for a Pay by Link Transaction) or Citi Mobile, Authentication for Authorization Purposes shall be effected by way of logging in to Citibank Online or Citi Mobile, entering (or confirming – in the case of Pay by Link Transactions) the details of the Payment Instruction and confirming the execution of the Payment Instruction by selecting the relevant function button used to submit the Payment Instruction to the Bank and by entering the relevant Authentication Code or performing a Mobile Authentication (including based on an Authentication Code) – if the Bank requires Strong Authentication, (b) the CitiPhone Telephone Banking Service, Authentication for Authorization Purposes shall be effected by way of entering the Card number and confirming it with the CitiPhone PIN or by way of CitiPhone PIN confirmation only where the Customer has enabled the Incoming Call Identification Service, (c) a Branch – Authentication for Authorization Purposes shall be effected after the identity of the Customer/Authorized User has been verified against a document that confirms their identity, or by entering the PIN, and, then, by confirming the Payment Instruction with a signature or the PIN.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Clarification of the provision relevant to the implementation of the Electronic Document Service Act (Journal of Laws, item 2320, and Journal of Laws 2021, items 72, 802, 1135, 1163 and 1598).	
Pre-amendment wording	**Post-amendment wording**
§ 13.14. The Bank shall accept complaints from Customers: (a) in written form – on a document submitted personally at a Bank Branch during the working hours of the Branch or sent to the following address: Citi Handlowy, Biuro Obsługi Reklamacji i Zapytań Klientów [Customer Complaint and Inquiry Office], ul. Goleszowska 6, 01-260 Warszawa 42; (b) in oral form – made by phone or personally for the record during the Customer's visit at a Bank Branch; (c) in electronic form – via the Citibank Online Service after logging in on the webpage under the "Contact the Bank" tab or through an email message to the Bank's e-mail address: listybh@citi.com, or a message to the Bank's Electronic Delivery Address AE: PL-51087-16873-WFBWS-31. The up-to-date contact details for submitting complaints are available on the Bank's website (www.online.citibank.pl)	§ 13.14. The Bank shall accept complaints from Customers: (a) in written form – on a document submitted personally at a Bank Branch during the working hours of the Branch or sent to the following address: Citi Handlowy, Biuro Obsługi Reklamacji i Zapytań Klientów [Customer Complaint and Inquiry Office], ul. Goleszowska 6, 01-260 Warszawa 42, or sent to the Bank's Electronic Delivery Address AE: PL-51087-16873-WFBWS-31. (b) in oral form – made by phone or personally for the record during the Customer's visit at a Bank Branch; (c) in electronic form – via the Citibank Online Service after logging in on the webpage under the "Contact the Bank" tab or through an email message to the Bank's e-mail address: listybh@citi.com. The up-to-date contact details for submitting complaints are available on the Bank's website (www.online.citibank.pl).

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Clarifying the provisions regarding the actions of the Customer and of the Bank if a Payment Instrument is blocked.	
Pre-amendment wording	**Post-amendment wording**
§ 14.2. Neither the Card, nor the User Name may be kept together with the Identification Code. § 14.3. The Card, the User Name, the Identification Code and the BLIK Code must not be made available to any third parties, and, in particular, they must not be made available for the purpose of effecting a Transaction or submitting a Payment Instruction at the CitiPhone Telephone Banking Service, Citibank Online or at a Branch.	§ 14.2. The Customer/Authorized User shall store the Payment Instrument, Username and PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password with due care and by observing the security rules set out in these Terms and Conditions, e.g. shall not store the Payment Instrument together with the User Name and PIN, ePINe, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password, shall not write down or record the User Name and PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2 /CVC2, 3D Secure Passwords in any form and on any medium or device, including on paper, on a phone (including the notes app and contact list), other multifunction device or computer. § 14.3. The Customer/Authorized User shall:

	(a) keep the Payment Instrument, User Name, PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password secret and shall not share them with third parties, in particular for the purpose of making a Transaction or placing a Payment Instruction in CitiPhone Telephone Banking Service, in Citibank Online or at a Branch, especially during a telephone call, even if the interlocutor introduces himself/herself as a Bank employee, an official (e.g. Police officer) or a close person; (b) not install software from received links or during a telephone call regarding the Customer's account or funds held in it, not click on links or attachments sent in e-mails, text messages or instant messengers if the Customer/Authorized User is not certain that they come from a verified sender, and shall not disclose the Payment Instrument, User Name, PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password on websites or applications accessed through links sent by unknown or unverified persons, including websites or applications featuring the Bank's graphic symbols; (c) not to provide the Payment Instrument, User Name, PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password in order to receive a payment in the case of remote Transactions without physically presenting the Card.
§ 17.19. When logging in to Citibank Online, the Customer should use equipment protected with a firewall helpful in protecting the computer against online attacks.	§ 17.20. The Customer/Authorized User undertakes to log in and make instructions via Citibank Online only in person. When logging in to Citibank Online, the Customer should use equipment protected with a firewall helpful in protecting the computer against online attacks.
§ 17.26. The Customer shall: (a) not share the BLIK Code, other Authorization Codes, Identification Codes, CVC2 number with third parties, (b) use the BLIK code, other Authorization Codes and Identification Codes in correspondence to their intended purpose, (c) immediately report to the Bank any unauthorized use of the BLIK Code, other Authorization Codes, Identification Codes by a third party.	§ 17.27. The Customer shall: (a) use the Payment Instrument in accordance with these Terms and Conditions, (b) store the Payment Instrument and Mobile Device with due care and security principles provided for in these Terms and Conditions, (c) install applications from authorized online application stores, such as Google Play and AppStore, (d) log in and place instructions via the Payment Instrument only in person, (e) not keep the Payment Instrument together with the PIN, CitiPhone PIN, Contactless Medium PIN, Citi Mobile Token PIN, ePIN, (f) not write down or record the PIN, CitiPhone PIN, Contactless Medium PIN, Citi Mobile Token PIN, ePIN, codes generated using Citi Mobile Token in any form or on any medium or device, including paper, telephone (including the notes app and contact list), another multifunction device or computer, (g) not make the Payment Instrument, Mobile Device, User Name, PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password available to unauthorized persons, third parties, including close persons, Bank employees or persons who introduce themselves as Bank employees, close relatives or state officials (e.g. Police officers), (h) not use applications or programs enabling remote access to the device (so-called remote desktop) where the Citi Mobile application is installed while simultaneously using Citi Mobile, (i) not use applications or programs enabling remote access to the device (so-called remote desktop) while logging in to the Citibank Online electronic banking service via a web browser installed on a mobile device or on a computer, (j) keep the PIN, CitiPhone PIN, Contactless Carrier PIN, Citi Mobile Token PIN, ePIN secret and

	not disclose it to third parties, especially during a telephone call, even if the interlocutor introduces himself/herself as a Bank employee, an official (e.g. Police officer) or a close person, (k) not install software from received links or during a telephone call, shall not click on links or attachments sent in e-mails, text messages or instant messengers if the Customer/Authorized User is not certain that they come from a verified sender, and shall not disclose the PIN, CitiPhone PIN, PIN Contactless Medium, Citi Mobile Token PIN, ePIN, Citicard PIN, Credit Card PIN on websites or applications accessed through links sent by unknown or unverified persons, including websites or applications featuring the Bank's graphic symbols, (l) read carefully any communications and messages warning against fraud and risks to the security of payment services, issued and sent by the Office of Competition and Consumer Protection (on https://uokik.gov.pl/), by the Polish Financial Supervision Authority (on https://www.knf.gov.pl/) and by the Bank on the Bank's website (https://www.citibank.pl/uslugi-online/bezpieczenstwo/), via Citi Mobile, Citibank Online, or via CitiPhone and shall contact the Bank in case of any doubts or problems with understanding specific communications or messages, (m) read carefully any messages received from the Bank via Citibank Online, Citi Mobile, SMS messages and e-mail in order to understand the nature of the instruction submitted to the Bank or the nature of the requested Transaction, as well as report to the Bank any irregularities noticed by the Customer in this respect, (n) use non-obvious combinations of characters when assigning a PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, 3D Secure Password (the use of character strings such as: 1111, 0000, 1234, 4321 is prohibited), in which connection the Bank shall inform the Customer that a given combination is not accepted when the latter is attempting to assign it; additionally, such combinations cannot refer to the Customer's date of birth, PESEL number, identity document numbers, telephone number, or other personal information of the Customer. (o) periodically update the PIN, ePIN, CitiPhone PIN, Citi Mobile Token PIN, BLIK Code, CVV2/CVC2, and 3D Secure Password.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Clarification of the provision regarding the Bank's procedure for handling complaints related to unauthorized Transactions	
Pre-amendment wording	**Post-amendment wording**
§ 14.12. The Customer will be charged with any Transactions made by persons to whom the Customer/User has made the Card available or has disclosed the Identification Code, subject to the provisions below.	deleted
§ 14.16. The Customer shall be liable for unauthorized Payment Transactions in the full amount if he/she led to them intentionally or as a result of intentional or grossly negligent violation of the rules	§ 14.16. In the case of an unauthorized payment transaction, the Bank shall refund the amount of such unauthorized payment transaction to the Customer immediately, but no later than by the

of use of the Card, BLIK Code, CitiPhone Telephone Banking Service or Citibank Online under the terms of the Agreement or failure to promptly report to the Bank the discovery of loss, theft or misappropriation of the Payment Instrument or unauthorized use of or access to the Payment Instrument, Identification Code, BLIK Code or device with which he/she receives Authorization Codes, BLIK Codes or performs Mobile Authentication or Citibank Online Authentication.	end of the business day following the day of detecting the unauthorized transaction charged to the Card Account or following the day of receiving the relevant report, except where the Bank has good and duly documented reasons to suspect a fraud, and the Bank shall notify law enforcement authorities of the same in writing. The Bank shall restore the debited Card Account to the balance that would have existed if the unauthorized transaction had not been made. Unless the Customer reports unauthorized transactions to the Bank within 13 months of the date of debiting the Card Account, the Customer's claims against the Bank due to unauthorized payment transactions shall expire. If an unauthorized payment transaction has been initiated through a Third Party Provider, the Bank shall immediately, but no later than the end of the business day following the date on which the unauthorized payment transaction debited to the Card Account was identified or following the day when it received the relevant report, restore the Card Account balance that would have existed if the unauthorized payment transaction had not occurred on the day .
§ 14.21. If after learning about or identifying an unauthorized payment transaction, the Bank credited the Card Account with a specific amount or restored the Card Account balance that would have existed if the unauthorized transaction had not taken place, and then, the Bank confirmed through an enquiry that the transaction had been authorized or the Bank found that the Customer was fully liable for the unauthorized transaction, the Bank shall, on the day of rejecting the complaint, re-debit the Card Account with the amount previously credited or with a relevant portion thereof.	§ 14.20. If the Bank has made, as per Clause 16 above, the refund of the amount of a Transaction identified or reported as an unauthorized payment transaction or has restored the Card Account balance that would have existed if such a transaction had not taken place, the Bank may debit the Card Account with an amount constituting the equivalent of the amount refunded to the Customer or the relevant portion thereof, if as a result of further enquiry as per § 13.18.-§ 13.23 of the Terms and Conditions, the Bank: (a) confirms that the Customer authorized the Transaction, or (b) the Bank has good and duly documented reasons to suspect a fraud on the Customer's part, and the Bank will notify law enforcement authorities of the same in writing; or (c) confirms that the Customer reported the unauthorized payment transaction to the Bank after the lapse of 13 months from the date when the Card Account had been debited, or (d) confirms that the Customer is liable for an unauthorized Payment Transaction up to the Polish currency equivalent of EUR 50, in accordance with Clause 13 above, or (e) confirms that the Customer caused the unauthorized Payment Transaction intentionally or as a result of willful or grossly negligent violation of at least one of the obligations provided for in § 14.1.-§ 14.4. of the Terms and Conditions, § 17.27. of the Terms and Conditions or point 44 of the "Citi Mobile Application" Rules. The Bank may debit the Card Account if at least one of the circumstances indicated in points (a)-(e) above applies. § 14.21. Having completed an enquiry if at least one of the circumstances indicated in Clause 20(a)-(e) above applies, the Bank, along with giving a negative response to the complaint, will request the Customer to return the amount transferred to the Customer under Clause 16 above, within the time-limit specified in the request, no less than 14 days. If the amount is not returned within the time-limit specified in the request, the Bank may debit the Card Account as per Clause 20 above after the lapse of the time-limit to no effect.
none	§ 14.23. If the Bank has not provided the Customer with appropriate means of prompt reporting at all times of a loss, theft, misappropriation or unauthorized use of the Card or other Payment Instrument or unauthorized access to the Card or other Payment Instrument, the Customer shall not be liable for unauthorized Transactions, unless the Customer has intentionally caused an unauthorized Transaction.

Terms and Conditions of Citibank Credit Cards	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (a) an amendment to or introduction of new laws and regulations applicable to the banking and/or financial sector or an amendment to any recommendations, guidelines or good practices by any institution supervising or linked to the banking sector relevant to the mutual rights and obligations of the parties to the Agreement.	
Factual background behind the amendment: Revis the wording further to the change of definition from "Authorization Code" to "Authentication Code".	
Pre-amendment wording	**Post-amendment wording**
§ 14.16. The Customer shall be liable for unauthorized Payment Transactions in the full amount if he/she led to them intentionally or as a result of intentional or grossly negligent violation of the rules of use of the Card, BLIK Code, CitiPhone Telephone Banking Service or Citibank Online under the terms of the Agreement or failure to promptly report to the Bank the discovery of loss, theft or misappropriation of the Payment Instrument or unauthorized use of or access to the Payment Instrument, Identification Code, BLIK Code or device with which he/she receives Authorization Codes, BLIK Codes or performs Mobile Authentication or Citibank Online Authentication.	§ 14.15. The Customer shall be liable for unauthorized Payment Transactions in the full amount if he/she led to them intentionally or as a result of intentional or grossly negligent violation of the rules of use of the Card, BLIK Code, CitiPhone Telephone Banking Service or Citibank Online under the terms of the Agreement or failure to promptly report to the Bank the discovery of loss, theft or misappropriation of the Payment Instrument or unauthorized use of or access to the Payment Instrument, Identification Code, BLIK Code or device with which he/she receives Authentication Codes, BLIK Codes or performs Mobile Authentication or Citibank Online Authentication.
§ 15.1. The Bank has the right to block a Payment Instrument: (a) on objective reasonable grounds linked to the security of the Payment Instrument; or (b) in connection with suspected unauthorized use of the Payment Instrument or suspected intent to effect an unauthorized payment transaction; or (c) if there is increased risk that the Customer may lose their creditworthiness required for a given Payment Instrument (only the possibility of making transactions will be blocked); or (d) in the case of Citi Mobile – after three failed attempts to use the Payment Instrument by providing an Authorization Code. The blockade is temporary and in effect until the Customer re-registers with Citi Mobile or; (e) in the case of a Card, to the exclusion of the Virtual Card, after three failed attempts to use the Card by providing an Authorization Code. The blockade is temporary and in effect until the Card is unblocked by the Customer. In such a case, it shall still be possible to execute Payment Instructions that do not require the provision of an Identification Code; or (f) in the case of CitiPhone – after three failed attempts to use the Payment Instrument by providing an Identification Code. The blockade is temporary and in effect until a new Identification Code to CitiPhone is provided; or (g) in the case of Citibank Online – after three failed attempts to use the Payment Instrument by providing an Authorization Code. The blockade is temporary and in effect until the Customer re-registers with Citibank Online, or (h) in the case of 3d Secure Authentication – after five unsuccessful attempts to Authenticate the Transaction. The blockade is temporary and applies only to Transactions made over the Internet using 3D Secure Authentication and lasts until the Customer/User reassigns an ePIN. In such a case, it is still possible to make Payment Instructions that do not require an 3D Secure Authentication or (i) in the cases provided for by applicable laws, according to the procedure and rules set forth in the Anti-Money Laundering and Countering the Financing of Terrorism Act of 1 March 2018.	§ 15.1. The Bank has the right to block a Payment Instrument: (a) on objective reasonable grounds linked to the security of the Payment Instrument; or (b) in connection with suspected unauthorized use of the Payment Instrument or suspected intent to effect an unauthorized payment transaction, or (c) if there is increased risk that the Customer may lose their creditworthiness required for a given Payment Instrument (only the possibility of making transactions will be blocked); or (d) in the case of Citi Mobile – after three failed attempts to use the Payment Instrument by providing an Authentication Code. The blockade is temporary and in effect until the Customer re-registers with Citi Mobile or; (e) in the case of a Card, to the exclusion of the Virtual Card – after three failed attempts to use the Card by providing an Authentication Code. The blockade is temporary and in effect until the Card is unblocked by the Customer. In such a case, it shall still be possible to execute Payment Instructions that do not require the provision of an Identification Code; or (f) in the case of CitiPhone – after three failed attempts to use the Payment Instrument by providing an Identification Code. The blockade is temporary and in effect until a new Identification Code to CitiPhone is provided; or (g) in the case of Citibank Online – after three failed attempts to use the Payment Instrument by providing an Authentication Code. The blockade is temporary and in effect until the Customer re-registers with Citibank Online, or (h) in the case of 3d Secure Authentication – after five unsuccessful attempts to Authenticate the Transaction. The blockade is temporary and applies only to Transactions made over the Internet using 3D Secure Authentication and lasts until the Customer/Authorized User reassigns an ePIN. In such a case, it is still possible to make Payment Instructions that do not require an 3D Secure Authentication or (i) in the cases provided for by applicable laws, according to the procedure and rules set forth in the Anti-Money Laundering and Countering the Financing of Terrorism Act of 1 March 2018.

§ 17.24. Neither the Bank nor its employees will ask for: (a) Identification Codes; (b) the CVC2 number placed on the Credit Card; (c) Authorization Codes. (d) BLIK Codes.	§ 17.25. Neither the Bank nor its employees will ask for: (a) Identification Codes; (b) the CVC2 number placed on the Credit Card; (c) Authentication Codes; (d) BLIK Codes.
§ 18.4. If a Payment Instruction or another activity carried out by the Customer using Citibank Online requires Strong Authentication, the Customer should verify the data sent in the text message containing the Authorization Code against the data entered in Citibank Online or Citi Mobile or verify the Payment Instruction as part of the Mobile Authentication (including based on an Authorization Code) or Citibank Online Authentication.	§ 18.4. If a Payment Instruction or another activity carried out by the Customer using Citibank Online requires Strong Authentication, the Customer should verify the data sent in the text message containing the Authentication Code against the data entered in Citibank Online or Citi Mobile, or verify the Payment Instruction as part of the Mobile Authentication (including based on an Authorization Code) or Citibank Online Authentication.

Terms and Conditions of Citibank Credit Cards

In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of:

(b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.

Factual background behind the amendment: Update of the guidelines for the provision of Citibank Online services in terms of unavailability and minimum criteria for using the website

Pre-amendment wording	Post-amendment wording
none	§ 17.10. The Bank provides the Customer with access to Citibank Online and Citi Mobile. Any planned service work related to the maintenance and development of Citibank Online and Citi Mobile shall be communicated in advance on the respective websites with the day and time of the planned unavailability specified. In the event of a failure, the Bank undertakes to remove any difficulties in using the online channels as soon as possible.
§ 17.13. In order to use Citibank Online and Citi Mobile, the Customer needs appropriate devices, hardware and software, including: (a) access to a computer or another device with an operating system supporting popular web browsers, e.g. Internet Explorer, Google Chrome, Mozilla Firefox; (b) enabled cookies and javascript (the device configuration manual is available on the website www.citihandlowy.pl); (c) enabled TLS 1.0 and 1.2; (d) Adobe Acrobat Reader version 9.0 or newer installed to handle PDF files; (e) Internet connection with the data transfer speed of at least 128 kb/s per workstation; (f) having open http (80) and https (443) ports.	§ 17.13. In order to use Citibank Online and Citi Mobile, the Customer needs appropriate devices, hardware and software, including: (a) access to a computer or another device with an operating system supporting popular web browsers, e.g. Google Chrome, Mozilla Firefox; (b) enabled cookies and javascript; (c) enabled TLS 1.0 and 1.2; (d) Adobe Acrobat Reader version 9.0 or newer installed to handle PDF files; (e) Internet connection with the data transfer speed of at least 128 kb/s per workstation; (f) having open http (80) and https (443) ports.

Terms and Conditions of Citibank Credit Cards

In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of:

(b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.	
Factual background behind the amendment: Update of provisions regarding the operation of a product	
Pre-amendment wording	**Post-amendment wording**
§ 23.10. All installments under the Plan shall be equal, apart from the first installment, which may cover a different amount, depending on how much time is left until the end of the settlement period. The Bank shall notify the Customer of the monthly Plan installment amount in the forthcoming Statement.	§ 23.10. All installments under the Plan shall be equal, apart from the first installment, which may cover a different amount, depending on how much time is left until the end of the settlement period, and the last installment, which settles the outstanding amount. The Bank shall notify the Customer of the monthly Plan installment amount in the forthcoming Statement.
Table of Fees and Commissions	
In accordance with § 28.1 of the Terms and Conditions of Citibank Credit Cards, the Bank is authorized to unilaterally amend the Agreement, including these Terms and Conditions, exclusively due to important reasons, in the case of: (b) a change in the scope or manner of rendering services, to which the provisions of these Terms and Conditions apply, by introducing new products or withdrawing existing services or changing their characteristics, provided that the change does not infringe the Customer's interests.	
Factual background behind the amendment: Increase in the chargeable amount of overpayment on the Card Account	
Pre-amendment wording	**Post-amendment wording**
Monthly fee for handling overpayments in the Credit Card account charged in the case the account shows in the settlement cycle a positive balance of or exceeding PLN 200	Monthly fee for handling overpayments in the Credit Card account charged in the case the account shows in the settlement cycle a positive balance of or exceeding PLN 300

The numbering and references in the Terms and Conditions of Credit Cards have been adjusted.