You will find revisions to particular documents in the table below.

Terms and Conditions of Citibank Credit Cards

Reason for revision (legal basis):
Pursuant to § 25 (1) of the Terms and Conditions of Credit Cards the Bank shall be 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 form of provision of services to which the provisions of these Terms and Conditions apply by the introduction of new products or withdrawal or change in characteristics of existing services, unless the change infringes on the Client's interests.

Factual basis for the revision: The following revisions to the Terms and Conditions of Credit Cards arise from adoption of a new authentication method for transactions without physical use of cards via the Internet.

Prior to revision	After revision
§ 1 (26) Authorization Code – a one-time code generated by the Bank for the purpose of authentication, including strong authentication, of a Transaction or an activity performed by the Client/User in Citibank Online, Citi Mobile, CitiPhone telephone banking or at a Branch.	§ 1 (26) Authorization Code – a one-time code generated by the Bank for the purpose of authentication, including strong authentication, of a Transaction or an activity performed by the Client/User in Citibank Online, Citi Mobile, CitiPhone telephone banking, at a Branch or online.
No definition.	§ 1 (86) Citibank Online Authentication – authentication of specific Transactions or non-cash Transactions made without physical use of the Card via the Internet, including electronic Client/User identification in Citibank Online by entering the User Name and the Identification Code and the Authorization Code from a text message received.
§ 7 (24) In the case of Transactions made remotely, without physical presentation of a Card (effected by telephone, in writing or via the Internet), a Transaction shall be deemed authorized through the provision of data of the Card or the Client/User, depending on the requirements of the Recipient, including the first and last name, the Identification Code, the number and expiry date of the Card or the CVV2/CVC2 code and authorization of the Transaction (if so required by the Bank) with an Authorization Code or using Mobile Authentication, Screen Unlock Method or Biometric Method.	§ 7 (24) In the case of Transactions made remotely, without physical presentation of a Card (effected by telephone, in writing or via the Internet), a Transaction is authorized by way of provision of Card or Client/User details, depending on the Recipient's requirements, including the first and last name, the Identification Code, the Card number and expiry date or the CVV2/CVC2 code, and authorization of the Transaction (if so required by the Bank) with an Authorization Code or Citibank Online Authentication or mobile Authentication, or by the Screen Unlock Method or the Biometric Method.
§ 7 (26) The Bank shall enable the Client to use an online Transactions protection in the form of 3D Secure Service or using Mobile Authentication. In the event where the Recipient of the Transaction made via the Internet requires additional verification a 3D Secure Password may have to be entered or the Transaction may have to be confirmed through Mobile Authentication in order to be executed.	§ 7 (26) The Bank allows Clients to secure online Transactions with 3D Secure or Mobile Authentication or Citibank Online Authentication. In the event where the Recipient of the Transaction made via the Internet requires additional verification a 3D Secure Password may have to be entered or the Transaction may have to be confirmed through Mobile Authentication or Citibank Online Authentication in order to be executed.
§ 13 (16) The Client shall be liable for any unauthorized payment Transactions in their full amounts if the Client caused such Transactions deliberately or as a result of willful or grossly negligent breach of the rules governing the Card, CitiPhone, or Citibank Online service as specified in the Agreement, or by failing to notify the Bank immediately about a loss, theft, appropriation or unauthorized use of the Card, CitiPhone or Citibank Online, the device by means of which the Client receives Authorization Codes or performs Mobile Authentication, or unauthorized access to the Card or the Identification Code, or CitiPhone or Citibank Online service or the device by means of which the Client receives Authorization Codes or performs Mobile Authentication	§ 13 (16) The Client shall be liable for any unauthorized payment Transactions in their full amounts if the Client caused such Transactions deliberately or as a result of willful or grossly negligent breach of the rules governing the Card, CitiPhone or Citibank Online service as specified in this Agreement, or by failing to notify the Bank immediately about a loss, theft, appropriation of the payment Instrument or unauthorized use or access to the payment Instrument, Identification Code or the device by means of which the Client receives Authorization Codes or performs Mobile Authentication or Citibank Online Authentication.

§ 16 (27) In the event of loss, theft, appropriation or unauthorized use of or access to the device used by a Client for access to Citibank Online or Citi Mobile (e.g. a computer, tablet, telephone or a similar device used for Mobile Authentication), especially if the circumstances justify a suspicion that the security of a Payment Instrument has been compromised, the Client should immediately notify such situation to the Bank via CitiPhone telephone banking service (by calling (+48) 22 692 24 84) or at the Bank's Branch to block that Payment Instrument. Notifications referred to in this Clause 27 shall be made for the Client free of charge.	§ 16 (27) In the event of a loss, theft, appropriation or unauthorized use of or access to the device used for Mobile Authentication or Citibank Online Authentication or use of Citibank Online or Citi Mobile, especially if the circumstances justify a suspicion that Payment Instrument security has been compromised, the Client should immediately report that fact in order to have the Payment Instrument blocked by calling CitiPhone at (+48) 22 692 24 84 or in person at a Branch. Notifications referred to in this Clause 27 shall be made free of charge.
§ 17 (4) If a Payment Order or another activity performed by the Client in Citibank Online requires Strong Authentication, the Client should verify the data sent in the SMS text message with the Authorization Code against the data entered in Citibank Online or Citi Mobile, or verify Payment Order details through Mobile Authentication (including with the use of the Authorization Code).	§ 17 (4) If a Payment Order or another activity performed by the Client in Citibank Online requires Strong Authentication, the Client should verify the data sent in the SMS text message with the Authorization Code against the data entered in Citibank Online or Citi Mobile, or verify Payment Order details through Mobile Authentication (including with the use of the Authorization Code) or Citibank Online Authentication.

Terms and Conditions of Citibank Credit Cards

Reason for revision (legal basis):
Pursuant to § 25 (1) of the Terms and Conditions of Credit Cards the Bank shall be 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 form of provision of services to which the provisions of these Terms and Conditions apply by the introduction of new products or withdrawal or change in characteristics of existing services, unless the change infringes on the Client's interests.

Factual basis for the revision: The following revisions to the Terms and Conditions of Credit Cards result from clarification of the provisions on transaction authorization via Google Pay and Apple Pay, and editorial changes in those provisions.

Prior to revision	After revision
§ 1 32) Biometric Method – the process of verifying the identity of a Mobile Device user by scanning characteristic points – a fingerprint, iris or a face map with a reader built into the Mobile Device.	§ 1 32) Biometric method – verification of the Client/User identity in a Mobile Device by way of verifying the Client's/User's unique features – fingerprint, iris or face map through an appropriate functionality available in the Mobile Device;
§ 1 33) Screen Unlock Method – a method of unlocking the screen of a Mobile Device based on User's knowledge.	§ 1 33) Mobile Device unlocking method – the method of unlocking a Mobile Device based on the Client's/User's knowledge.
§ 1 84) Mobile device – a device with Internet access, iOS or Android operating system.	§ 1 80) Mobile device – a device with Internet access, iOS, iPadOS, macOS or Android operating system.
§ 7 (16) Save for Transactions made in the manner specified in § 7 (22) to (24), and (36) below or a Transaction made as a result of concluding the Understanding referred to in § 20 (9) to (11) below, a Transaction made with a Card is deemed authorized by the Client/User if it has been confirmed by using the PIN number, Screen Unlock Method or Biometric Method, or affixing the signature of the Client/User on the debit document in accordance with the signature affixed on the Card or the Specimen Signature, in case strong authentication is not required. By authorizing a Transaction, the Client/User approves debiting of the Card Account with the amount of such a Transaction plus the fees and commissions as per the Table of Fees and Commissions.	§ 7 (16) Save for Transactions made in the manner specified in § 7 (22) to (24), and (36) below or a Transaction made as a result of concluding the Understanding referred to in § 20 (9) to (11) below, a Transaction made with a Card is deemed authorized by the Client/User if it has been confirmed by using the PIN number, Mobile Device Unlock Method or Biometric Method, or affixing the signature of the Client/User on the debit document in accordance with the signature affixed on the Card or the Specimen Signature, in case strong authentication is not required. By authorizing a Transaction, the Client/User approves debiting of the Card Account with the amount of such a Transaction plus the fees and commissions as per the Table of Fees and Commissions.
§ 7 (18) An ATM cash withdrawal using a Card is considered authorized if it has been confirmed with a PIN or the Screen Unlock Method or the Biometric Method. A cash withdrawal from an ATM by means of a Card in Poland or abroad is subject to restrictions provided by applicable laws.	§ 7 (18) An ATM cash withdrawal using a Card is considered authorized if it has been confirmed with a PIN or the Mobile Device Unlock Method or the Biometric Method. A cash withdrawal from an ATM by means of a Card in Poland or abroad is subject to restrictions provided by applicable laws.

§ 7 (22) In the case of a contactless Transaction: a) equal to or above the Contactless Transactions Value Limit or in the cases specified in §7 (56) below, a Transaction is considered authorized if it has been confirmed with a PIN or the Screen Unlock Method or the Biometric Method. Moreover, in cases where the Bank does not require strong authentication, the Transaction is deemed authorized by the Client/User signing a debit note consistently with the signature on the Card; b) below the Contactless Transaction Value Limit – the Transaction shall be deemed authorized upon delivery of the details of the Card or Contactless Medium saved in the Contactless Module that are required to execute the Transaction, by putting the Card or Contactless Medium in the proximity of the device that enables reading the data saved in the Contactless Module. In the cases specified in §7 (56) below, a Transaction is considered authorized if confirmed with a PIN or the Screen Unlock Method or the Biometric Method; c) in the cases of a contactless Transaction other than those specified in clause a) and b) above, where the Bank, under the applicable law, is not obliged to use strong authentication, the Transaction is deemed authorized upon transfer of the data of the Card or the Contactless Medium that are saved in the Contactless Module and are required to execute a Transaction, by putting the Card or the Contactless Medium close to the device enabling the readout of data saved in the Contactless Module.	§ 7 (22) In the case of a contactless Transaction: a) equal to or above the Contactless Transactions Value Limit or in the cases specified in §7 (56) below, a Transaction is considered authorized if it has been confirmed with a PIN or the Mobile Device Unlock Method or the Biometric Method. Moreover, in cases where the Bank does not require strong authentication, the Transaction is deemed authorized by the Client/User signing a debit note consistently with the signature on the Card; b) below the Contactless Transaction Value Limit – the Transaction shall be deemed authorized upon delivery of the details of the Card or Contactless Medium saved in the Contactless Module that are required to execute the Transaction, by putting the Card or Contactless Medium in the proximity of the device that enables reading the data saved in the Contactless Module. In the cases specified in §7 (56) below, a Transaction is considered authorized if confirmed with a PIN or the Mobile Device Unlock Method or the Biometric Method; c) in the cases of a contactless Transaction other than those specified in clause a) and b) above, where the Bank, under the applicable law, is not obliged to use strong authentication, the Transaction is deemed authorized upon transfer of the data of the Card or the Contactless Medium that are saved in the Contactless Module and are required to execute a Transaction, by putting the Card or the Contactless Medium close to the device enabling the readout of data saved in the Contactless Module.

Terms and Conditions of Citibank Credit Cards

Reason for revision (legal basis):
Pursuant to § 25 (1) of the Terms and Conditions of Credit Cards the Bank shall be 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 form of provision of services to which the provisions of these Terms and Conditions apply by the introduction of new products or withdrawal or change in characteristics of existing services, unless the change infringes on the Client's interests.

Factual basis for the revision: The following revisions to the Terms and Conditions of Credit Cards result from clarification of the information on overpayments settlement after expiration of the Credit Card Agreement.

Prior to revision	After revision
No provision.	§ 8 (3) In the event of Agreement expiration, the Bank shall settle accounts with the Client within 14 days. Any overpayment shall be transferred by the Bank to the Client's account at the Bank or the account indicated by the Client in the manner specified in section 2 above or shall be made available to the Client for cash withdrawal at a Branch.

Terms and Conditions of Citibank Credit Cards

Reason for revision (legal basis):
Pursuant to § 25 (1) of the Terms and Conditions of Credit Cards the Bank shall be 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 form of provision of services to which the provisions of these Terms and Conditions apply by the introduction of new products or withdrawal or change in characteristics of existing services, unless the change infringes on the Client's interests.

Factual basis for the revision: The following revisions to the Terms and Conditions of Credit Cards arise from clarification of the information about the number of possible attempts to use the 3D Secure Password to confirm Transactions made via the Internet using 3D Secure.

Prior to revision	After revision
§ 14 1. The Bank has the right to block a Payment Instrument: a) for objectively justified reasons, tied to the safety of Payment Instrument, or b) due to a suspicion of unauthorized use of the Payment Instrument or intentional action aimed at causing the execution of an unauthorized payment transaction, or c) if there is increased risk that the Client may lose their creditworthiness required for a given Payment Instrument (only the option of making transactions will be blocked), or d) for Citi Mobile, after three unsuccessful attempts to use the Payment Instrument using an authentication code. Such blockade is temporary and will last until the next time the Client signs on to Citi Mobile, or e) in the case of a card, after three unsuccessful attempts to use the Card using an authentication code. The blockade shall be temporary and will last until the Card is unblocked by the Client. In such a case, Payment Orders which do not require the Identification Code may still be executed, or f) for CitiPhone services, after three unsuccessful attempts to use the Payment Instrument using an authentication code. The lock is temporary and continues until a new Identification Code for CitiPhone banking service is assigned or g) for Citibank Online, after three unsuccessful attempts to use the Payment Instrument using an authentication code. The lock is temporary and continues until Client's next log-in to Citibank Online.	§ 14 (1) The Bank has the right to block a Payment Instrument: a) for objectively justified reasons, tied to the safety of Payment Instrument, or b) due to a suspicion of unauthorized use of the Payment Instrument or intentional action aimed at causing the execution of an unauthorized payment transaction, or c) if there is increased risk that the Client may lose their creditworthiness required for a given Payment Instrument (only the option of making transactions will be blocked), or d) for Citi Mobile, after three unsuccessful attempts to use the Payment Instrument using an authentication code. Such blockade is temporary and will last until the next time the Client signs on to Citi Mobile, or e) in the case of a card, after three unsuccessful attempts to use the Card using an authentication code. The blockade shall be temporary and will last until the Card is unblocked by the Client. In such a case, Payment Orders which do not require the Identification Code may still be executed, or f) for CitiPhone services, after three unsuccessful attempts to use the Payment Instrument using an authentication code. The lock is temporary and continues until a new Identification Code for CitiPhone banking service is assigned or g) for Citibank Online, after three unsuccessful attempts to use the Payment Instrument using an authentication code. Such blockade is temporary and will last until the next time the Client signs on to Citibank Online, or h) for a 3D Secure Password, after five unsuccessful attempts to use the Payment Instrument using that password. The lock is temporary and continues until 3D Secure is unlocked. In such a case, Payment Orders which do not require the 3D Secure Password may still be executed.

Terms and Conditions of Citibank Credit Cards

Legal and factual basis for the revisions: The following revisions to the Terms and Conditions of Credit Cards result from editorial corrections in the provisions concerning the terms of informing clients about total fees for currency translations for transactions in the currencies of the European Economic Area other than PLN where the payer's and payee's payment service providers are located in the European Economic Area.

Prior to revision	After revision
§ 7 (12) Exchange rates applied by the Payment Organization for translations of amounts of Transactions executed with a Citibank Credit Card into PLN are available on the website of the Bank https://www.citibank.pl/poland/homepage/polish/kursy-walut.htm along with the rules of their use. In the case of Card Transactions in currencies of the European Economic Area other than PLN, if payment service providers of the payer and the payee are located in the European Economic Area, the Bank shall, immediately after Transaction execution, provide the Client or the User with an email or text message stating total currency conversion charges as a percentage margin on the most recent euro reference exchange rate published by the European Central Bank. The information referred to in the preceding sentence shall also be sent by the Bank to the Client or the User via Citibank Online or by email once during the month in which the Bank received the payment order denominated in the currency referred to in the preceding sentence.	§ 7 (12) Exchange rates applied by the Payment Organization for translations of amounts of Transactions executed with a Citibank Credit Card into PLN are available on the website of the Bank https://www.citibank.pl/poland/homepage/polish/kursy-walut.htm along with the rules of their use. In the case of Card Transactions in currencies of the European Economic Area other than PLN, if payment service providers of the payer and the payee are located in the European Economic Area, the Bank shall, immediately after the Bank receives the Payment Instruction, provide the Client or the User with an email or text message stating total currency conversion charges as a percentage margin on the most recent euro reference exchange rate published by the European Central Bank. The information referred to in the preceding sentence shall also be sent by the Bank to the Client or the User via Citibank Online or by email once during the month in which the Bank received the payment order denominated in the currency referred to in the preceding sentence.

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