

General Conditions for Remote Communication Channel Services



Individual Customers

Clause 1. Scope

1. These General Conditions are meant to regulate the terms and conditions for the Customer to access the services mentioned above provided by the Bank through Remote Channels.

2. For the purposes of this contract, the following are considered remote communication channels between the Bank and the Customer:

a) Telephone Channel, hereinafter referred to as Contact Centre when it involves a call centre service - communication by phone established by initiative of the Bank or the Customer or of the Bank, including the phone contacts established through the Contact Centre (communications associated to phone numbers +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call) or other numbers that may replace them that are disclosed by the Bank). The cost of communications will depend on the rate you have agreed with your telecommunications operator. The Contact Centre is a permanent customer service (24 hours/day, 365 days/year);

b) Internet Channel - the Customer's access to the Bank's website at Internet www.millenniumbcp.pt;

c) Mobile Channel - the Customer's access to the Bank using Millennium App, MTrader App, Apple Watch and other extensions of the Apps;

d) Millennium Teller Machine, hereinafter referred to as MTM - selfbanking ATM machine for the Customer to access the Bank wherein the Customer can view account information, make cash/cheque banking operations and subscribe to financial products and services autonomously or with assistance (in person or remotely, being the latter made with Authentication Code).

3. The remote communication channels are channels enabling the Customer's remote access to the services that, at each moment, the Bank has available in those channels, for the celebration of legal acts and businesses within the scope of the bank relation established with the Bank, in its capacity as credit institution, financial intermediary and insurance agent, enabling the remote access to the current deposits account for consultation, obtaining information and making of operations, as well as for the disclosure and trade by the Bank, and remote contracting of financial products and services, including those related with payment services, financial instruments and insurances.

4. For the purposes of the preceding paragraph, legal acts or transactions entered into in the context of banking relationships shall be deemed to be all those relating to the opening, maintenance and closure of current accounts, payment services, credit services or the registration or deposit of financial instruments, the operation of such accounts, and the entering into and performance of life and non-life insurance contracts and the management of claims, including, in particular, the carrying out of insurance transactions, the issuance of powers of attorney, the issuance of statements relating to personal data, the submission of claims or various requests, the submission of requests for statements, requests for information, requests for duplicates of statements or other documents, the issuance of receipts, the signing of contracts for the use of payment instruments including payment instruments for secure e-commerce and dematerialised card-based transactions, requests for access codes or codes for the use of Internet services or payment instruments, the conclusion of acquiring and APT requisition contracts, the contracting of direct debits, the contracting of money remittance services, the issue and revocation of payment orders, including standing or periodic orders the issue of orders for the purchase, sale or redemption of financial instruments, even if on the stock exchange, the subscription or redemption of retail investment products and insurance-based investment products, the requisition of cheques, the purchase and sale of currency, the constitution, reinforcement or settlement of term deposits, the contracting and settlement of safe deposit boxes, the contracting or management of credit operations, leasing, the issue of guarantees.

5. Within the scope of remote communications, the Customer agrees to be approached at the Bank's initiative. In the case of the Telephone Channel, contacts will be made to the telephone numbers given by the Customer.

6. For the purposes of the previous paragraph, the Customer expressly consents and requests the Bank, through these remote communication channels, as well as by e-mail, to disclose and present concrete proposals for the signing or amendment of contracts, subscription to products and services and execution of operations made remotely of financial products and services, including banking services, payments, loans, intermediation or investment in financial instruments, individual application agreements for open pension funds, even if such proposals involve a payment request.

7. The Customer may add other current deposit accounts held by him/her with the Bank to the service provided by remote communication channels (aggregate accounts), but in the case of a collective account without autonomous handling powers

from the Customer, the provisions of the following paragraph of this clause and of clause 8, no. 7, below, shall apply in particular.

8. Without prejudice to other measures for restricting access that the Bank may apply, if the current deposits account or another linked account is a tenants-in-common account where the Customer does not have autonomous powers to use it, (i) access to the Internet, Mobile and MTM channel is limited to viewing and obtaining information, without access to execute operations, (ii) the use of the Contact Centre to execute operations implies a verification procedure under the terms of clause 8, no. 7.

9. Through the remote communication channels, the Customer may ask to purchase products or services with third party entities, under the terms of the agreement entered into between the latter and the Bank.

10. The provision of services by means of remote communication channels shall also be governed, in all matters not specifically provided for herein, by the provisions of Chapter A - General Conditions for Current Deposits Accounts and Chapter B - General Conditions for the Provision of Payment Services and Chapter C - General Conditions for Registration and Deposit of Financial Instruments and Financial Intermediation, all of the General Conditions for Current Deposits, which are hereby reproduced for all due purposes.

11. All contracts concluded through the remote communication channels are subordinated to these Contract and the general and specific conditions applicable to the contracting of each product or service specifically provided, as well as to the price list in force at the Bank, applicable legislation and bank use in general.

Clause 2. Risks associated with the remote communication channels

1. The remote communication channels for the Customer's access to the Bank are subject to the risks of fraud by third parties, namely phishing, as well as, consultation and execution of fraudulent transactions by unauthorised third parties on the Customer's account.

2. Phishing is a fraud consisting in substituting the identity of the Bank or any other trustworthy entity and whose purpose is to obtain confidential information of the Customer, namely bank details, personal details or access codes. Phishing attacks may be made through e-mails messages, short message services SMS or phone calls in which the identity of the Bank or any other trustworthy entity can be impersonated and replaced. These e-mails or SMS messages may contain an attached file that installs malicious software (malware) on the Customer's equipment or redirects to a fraudulent web page, which reproduces or copies the look and feel of the Bank's original page, and in which the Customer is requested to enter personal data and/or access codes and credentials, such as, for example, his/her User Code, some or all of the positions of his/her Multichannel Code, the Authentication Code, his/her mobile phone number or the Data of his/her bank cards;

3. The Customer must be alert, be cautious and bear in mind that both the fraudulent e-mail or SMS, as well as the fraudulent web page, can be very complex and sophisticated. The Customer must be wary and suspicious of, namely:

a) the urgency tone of messages threatening him/her with the suspension of access to his/her account, his/her access codes or bank card codes if he/she do not immediately provide his/her data;

b) the curiosity created by the message, which offers a much desired service or product;

c) the request for confirmation of his/her personal data via e-mail or SMS, in particular by referring him/her to the on line filing of personal data forms and access codes;

d) the spelling/grammatical errors, incomplete translations, errors in the sender's address (@domain)t and other errors evident in the message or in the fraudulent web page, or other elements that suggest their diverse or suspicious origin;

e) e-mails or SMS messages with links or files attached;

f) the indication that, in order to simulate/cancel operations, he/she must provide Authentication Code(s) that the Bank sent him/her by SMS or generated via Token.

4. The Bank is in charge of ensuring that its website, Mobile Banking and MTM services are reliable and that its servers and IT components are safe.

5. The Customer is responsible for the security and reliability of the IT and communication equipment used to access the Bank through remote communication channels, namely computers, tablets, mobile phones, mobile phone numbers and Internet connections owned by or under the control of the Customer, in accordance with the provisions of the following paragraphs and the security recommendations and rules set out in ATTACHMENT 1 - RISKS AND SAFETY RULES.

6. The Customer must possess IT and communications equipment with the appropriate characteristics to be able to access the Bank through remote communication channels, being his/her responsibility the security, maintenance, update and introduction of any modifications that may be required to ensure permanent access to the Bank through remote communication channels, according to the technological innovations and changes that may be introduced and strict compliance with the security rules and recommendations contained in ATTACHMENT 1 - RISKS AND SAFETY RULES, as well as the alerts disclosed by the Bank, at each moment, at the bank's website www.millenniumbcp.pt.

7. The minimum characteristics, in terms of equipment and communications, required at all times for the use of each remote communication channels are described on the Bank's website, in the information spaces of each channel, which the Customer undertakes to consult periodically and scrupulously observe.

Clause 3. Open Banking

It is herein expressly agreed and accepted that, according to the requirements of the Directive (EU) 2015/2366 of 25.03.2015 and the legal provisions that regulate it and transpose it, the Bank, under its capacity as the payment services provider that manages the current deposits account is obliged to provide the access to the said account available to third parties payment services providers, without the need of the establishment of any contractual relation between these and the Bank and provided that the Customer gives his/her consent for purposes of the provision of the services of accounts aggregation, payment initiation and balances confirmation, better described in ATTACHMENT 2 - OPEN BANKING and that are an integral part of this Contract.

Clause 4. Custom Security Credentials

1. A Multichannel Code for access to the Contact Centre, Internet, Mobile and MTM channels can be attributed to the Customer who expressly requests it from the Bank through the website www.millenniumbcp.pt, the Mobile channel, a Branch or a Multibanco ATM.

2. Access to the Internet, Mobile and MTM channels requires an additional User Code, which should be altered the first time the Customer logs on the website www.millenniumbcp.pt.

3. Access via Apple Watch to the current deposits account and other aggregated accounts is additionally subject to identification and recognition processes defined in separate contractual clauses.

4. Access to the MTM channel may additionally be made with a personalized bank card and correct introduction of the corresponding PIN.

5. The Bank requests, at the same time or for the same act, the input of only three (3) random positions of the Multichannel Code.

6. For the performance of certain legal acts or transactions on the remote communication channels, namely to carry out payment transactions above a certain amount executed by debiting the current deposits account or an aggregated account, additional confirmation may be required through (i) a Customer's Strong Authentication (CSA) system - prior confirmation of the transaction with biometric data or a single authorization code generated by Token or sent by SMS to the Customer's mobile phone number at the time of the transaction, which identifies the transaction data to be confirmed, or (ii) the transaction confirmation with some random positions of the Customer's Multichannel Code.

7. The Customer, through the available services, may, at any time, define and manage the payment operations that namely may cause a decrease in assets, and/or depending on the beneficiaries involved, will not require the use of the CSA for their execution.

8. The Bank may, at any given moment, define a series of conditions - namely concerning beneficiaries, amounts and/or operations - the verification of which may exempt the use of the additional CSA for their execution.

9. The Bank will not ask by phone, SMS or e-mail for information about the User Code and/or Authentication Code, or for his/her bank card or mobile phone details.

10. At www.millenniumbcpt.pt website, the Customer can change at any time the User Code as well as the Multichannel Code. The Multichannel Code can also be changed through the Contact Centre channel (only in automated service - Voice Response System) and the Mobile channel (security area).

11. To perform some transactions or to change personal data, additional security information (personal or relationship with the Bank) may be requested through a personalised telephone contact from the Contact Centre service.

Clause 5. Digital Mobile Key

1. In the Internet and Mobile Channels, exclusively for access and authentication regarding those channels, the Customer may choose, as an alternative to using the codes mentioned in the previous chapter, to use the Digital Mobile Key authentication service made available by the Portuguese State and sub-contracted by the Bank.

2. The Digital Mobile Key is a mean to access and authenticate that enables associating a mobile phone number to the civil identification number of a Portuguese citizen or the number of the passport for a foreign citizen residing in Portugal. The Digital Mobile Key enables the user to be authenticated through:

a) Mobile phone number;

b) PIN - Non-transferable personal identification number created at the registration of the Digital Mobile Key;

c) Unique and temporary 6-digit numeric security code sent by SMS to the Customer's mobile phone number or obtained via the "Gov Authentication" App;

3. By choosing any of these methods, the Customer is responsible for the safe use of the PIN as well as of the mobile phone associated to the registration;

4. Access to the Bank's Internet and Mobile channels using the Digital Mobile Key authentication requires the Customer's prior application on the autenticacao.gov.pt website or in person at *Espaços Cidadão*;

5. By selecting this form of authentication the Customer is redirected in a safe manner to the Internet service autenticacao.gov.pt, where he/she is informed of the data requested by the Bank and explicitly agrees with that transmission;

6. It is hereby expressly agreed that the user's authentication using the Digital Mobile Key gives the Bank the legitimacy to grant access to the chosen Internet or Mobile channel chosen and to the Customer's correspondent current deposits account(s).

Clause 6. Convention on proof

1. The Customer's access to and use remote communications channels, namely for carrying out payment transactions, transmitting orders and instructions, shall be subject to proper use, according to the provisions of these clauses and corresponding ATTACHMENT 1- RISKS AND SAFETY RULES:

a) Of the User Code, Multichannel Code and PIN (to access the Millennium App) and/or each single-use code that the Bank sends to the Customer's cell phone number indicated to the Bank for remote operations or generated by Token; and

b) The Customer's cell phone or mobile device with the mobile number previously provided to the Bank for remote operations and/or on which there is installed a Bank App or the MB Way App associated to a bank card; and

c) The Customer's e-mail address given to the Bank for the purposes of remote communication exchange and/or for the purposes of authentication before the Bank.

2. All the Customer's Codes and other elements and devices indicated in the preceding paragraph shall constitute personalised security credentials enabling the Bank to verify the Customer's identity, authenticate the Customer's access to and use of each remote channel and establish authorship of the orders transmitted therein, constituting an electronic signature which is the object of an individual and exclusive right of the Customer, the use of which identifies and authenticates the Customer before the Bank and attributes to the Customer authorship of the electronic instructions and documents thus transmitted.

3. The Parties accept the legal equivalence of the aforementioned personalised security credentials of the Customer, as well as the Mobile Digital Key, to the Customer's handwritten signatures.

4. The Bank shall legitimately assume that any access, information request, orders or instructions transmission, execution of a contract or execution of any legal acts or transactions using the aforementioned personalised security credentials, under the terms agreed herein, as well as the Mobile Digital Key, under the terms herein agreed, as being of the Customer's authorship, not being required to verify the user's identity by any other means.

5. The provisions set forth in the previous number cannot be interpreted as able to prevent the Bank from obtaining confirmation from the Customer concerning the orders or instructions received, including a written confirmation, with a handwritten signature, nor damage the adoption of another way to formalize the banking transactions at the Bank's request or due to a legal requirement, or limit the acceptance of a specific type of instructions in view of amounts, number of orders or other criteria.

6. The orders and instructions received by the Bank, as well as the subscription of contracts, or the execution of any legal acts or transactions, provided that they are correctly validated through the use of the aforementioned personalised security credentials or of the Mobile Digital Key, have full legal effect, and the Bank is irrevocably empowered to comply with them or to execute them and make the debits and credits resulting therefrom, it being understood, in any event, that the Bank is acting in compliance with the orders and instructions received and the real will of the Customer.

7. It is expressly agreed between the Customer and the Bank that, under the terms and for the purposes of paragraph 9 of art. 3 of Decree-Law 290-D/2021, of February 09, the use of the aforementioned personalised security credentials of the Customer, including each of the Authentication Codes assigned to the Customer, the Customer's mobile phone or mobile device with the mobile phone number previously indicated to the Bank for the execution of remote operations, as well as the Mobile Digital Key, under the terms hereby established, shall have the same legal and evidential value as the Customer's handwritten signature on paper.

8. The provisions of paragraphs 4 and 5 and of the present clause also apply to the contracting of products and services with third parties, provided for in clause 1 no. 9, with the Bank, within the scope of this provision, acting in the name and on behalf of those entities.

Clause 7. Customer's obligations concerning his/her personalised security credentials, mobile phone number and e-mail address

1. The Customer undertakes to take all reasonable care and diligence to preserve the security and confidentiality of his/her personalised security codes and credentials indicated in clause 6 (Agreement on proof) above, for the purposes of authentication before the Bank, and not to allow or facilitate their knowledge or use by third parties, even if acting as his/her representatives, and undertakes to maintain their confidentiality at all times and to make a careful, cautious, reserved and exclusively personal use of them.

2. The Customer is responsible for the correct confidentiality, safekeeping, use and maintenance of the User Code, Multichannel Code and PIN (for access to the Millennium App), well as the other personalized security elements and credentials referred to in clause 6 (Agreement on proof) above.

3. Namely, the Customer undertakes to take all appropriate precautions not to make the User Code and/or Multichannel Code accessible or noticeable to third parties, which he/she must memorize by destroying the respective information support of the same(s). If the Customer intends to keep the aforementioned codes, he/she must never leave them in a place that is visible, accessible and/or perceptible to third parties, and in particular must not write them down in a medium that is easily accessible to third parties, neither on his/her mobile phone, mobile device or computer, nor on any other document or medium that he/she has or near them.

4. The Customer must be aware, be cautious and bear in mind that there is a risk of receiving misleading e-mails, SMS or even telephone calls in which the identity of the Bank is imitated and replaced in order to cunningly and fraudulently obtain from the Customer his/her data, personal codes and access credentials, such as, for example, his/her User Code, (all) positions of his/her Multichannel Code, his/her mobile phone number, the numbers of his/her bank and/or Credit card(s) and should be suspicious and wary of the verification of any of the circumstances referred to in paragraph 3 of the preceding clause 2.

5. The Customer undertakes to read carefully and scrupulously comply with the security recommendations and rules contained in ATTACHMENT 1 - RISKS AND SAFETY RULES, as well as to consult and read, at least once every quarter of the calendar year, the security notices and periodic alerts that the Bank discloses on the Internet site www.millenniumbcp.pt, including the description of the specific procedure(s) used at each moment for the fraudulent capture of the User Code, Multichannel Code and other personalised access credentials of the Customers.

6. The Customer must never, under any circumstances, enter all the positions of his/her Multichannel Code at the same time or for the same act. The Bank never requests, at the same time or for the same act, the simultaneous or phased introduction of all the positions of the Multichannel Code.

7. The Customer also undertakes to take all reasonable precaution and diligence measures to safeguard and preserve:

a) The possession, security and exclusive, reserved and confidential use at all times of his/her mobile phone or mobile device with the mobile number previously provided to the Bank to perform remote transactions, and/or on which he/she has installed a Bank App or the MB Way App associated with a bank card;

b) The exclusive, reserved and confidential use at all times of the Customer's email address given to the Bank for the exchange of remote communications and/or for authentication purposes before the Bank.

8. If at any moment, the Customer:

a) Suspects that third parties have knowledge, in whole or in part, of his/her User Code and/or Multichannel Code, or in case of loss, theft or misappropriation of the same or any of them, and/or

b) Verifies the registration in the account of any not authorised transaction or the existence of errors or irregularities in the execution of transactions; and/or

c) Receives an Authentication Code to simulate /cancel a transaction; and/or

d) Receive an Authentication Code to confirm a transaction that the Customer has not requested; and/or

e) Suspects that a third party(ies) has(have) improper access to his/her email address and/or to his/her mobile phone or device or to his/her mobile phone number in any way,

The Customer must then suspend the procedure and, without undue delay, immediately contact the Bank through the Contact Centre channel at the numbers indicated in paragraph 2(a) of clause 1, in order to raise the alert and request the respective blocking/impediment of abusive or fraudulent use before the Bank. The Customer must also confirm the occurrence to the Bank, in writing, within a period not exceeding 5 days.

9. All cases under paragraphs a) to and) of the preceding number must be promptly reported to the competent police authorities, and the Customer must present the Bank with documentary evidence thereof, along with a copy of the contents of the report made.

10. The User Code or Multichannel Code shall not be used for the telephone communications referred to in the preceding paragraph 8 of this clause. In this case, the Customer declares and accepts that the Bank shall consider him/her as identified and acknowledged as soon as he/she cumulatively and correctly indicates the answer to the questions asked by the Bank regarding elements of the Customer's financial assets, deposit accounts belonging to him/her, or other facts that are known to the Bank by virtue of the respective customer relationship or others that have been previously agreed between the Parties for this purpose.

11. Following the Customer's communication referred to in the preceding paragraphs of this clause, the Bank shall block access to the Customer's accounts through the remote communication channels.

12.1. After proceeding without undue delay to the notification referred to in the preceding paragraph 8, the Customer shall not bear any losses relating to unauthorized payment transactions resulting from a breach of confidentiality of his personalized security codes and credentials indicated in clause 6 (Convention on proof), in particular in the event of loss, theft or misappropriation of the same or any of them, except those due to fraudulent action by the Customer.

12.2. The Customer shall bear the losses relating to unauthorised payment transactions resulting from a breach of confidentiality of the Customer's personalised security codes and credentials indicated in clause 6 (Agreement on proof), namely in the event of loss, theft or misappropriation of the same or any of them, which are carried out before the notification referred to in the preceding clause 8, in accordance with the following rules:

a) The Customer shall bear all losses resulting from unauthorised payment transactions if they are due to fraudulent behaviour or to wilful non-compliance with one or more of the Customer's obligations set out in this Agreement, in particular in the present clause and in ATTACHMENT 1 - RISKS AND SAFETY RULES, and if, in the event of suspected fraud, the Bank communicates these reasons in writing to the judicial authorities;

b) In the event of gross negligence on the part of the Customer, the Customer shall bear the losses resulting from unauthorised payment transactions up to the limit of the available balance or the credit line associated to the account, even if they exceed EUR 50;

c) In other cases, the Customer bears the losses relating to unauthorised operations, within the available balance or the credit line associated with the account, up to a maximum limit of EUR 50. This Customer responsibility does not apply if:

(i) The loss, misplacement, theft, improper access or other misappropriation of the Customer's personalised security codes and credentials indicated in clause 6 (Convention on proof) could not have been detected by the Customer before making a payment, unless the Customer has acted fraudulently; or

(ii) if the loss was caused by acts or omissions of an employee, agent or of a branch of the payment service provider, or of an entity to which its activities have been outsourced.

12.3. If the payment transaction was initiated through a payment initiation service provider, the burden shall be on the latter to prove that, within its sphere of competence, the payment transaction was authenticated and accurately recorded, and that it was not affected by a technical breakdown or other deficiency linked to the payment service provided.

12.4. Once the proof diligences mentioned in the previous number are concluded, if it appears that the Bank or the payment initiation services provider is responsible for the losses due to unauthorized operations, the Bank will ensure the reimbursement immediately and, in any event, the latest until the end of the following first working day, of the amount of the unauthorized payment operation and, if needed be, restore the Customer's account to the state in which it would have been had the unauthorised payment transaction not been executed, with a value date no later than the date the amount was debited.

Clause 8. Processing of the Customer's Instructions

1. Without prejudice to the provisions of clause 11 below, the Customer may give instructions to the Bank by means of remote communication channels at any time of the day, every day of the year and in person within the opening hours of the Bank's Branches.

2. The execution of the orders given by the Customer will be carried out according to the conditions applicable to the type of remote channel, service or product requested.

3. The Bank may refrain from executing orders transmitted by the Customer, when such orders do not comply with the applicable legal provisions or conflict with banking practices, when the account to be operated is not provided for the intended operation, or when any provision contained in this Agreement and/or in the provisions of Chapter A - General Conditions for Current Deposits Accounts is not complied with, Chapter B - General Conditions for the Provision of Payment Services and Chapter C - General Conditions for Accounts for the Registration and Deposit of Financial Instruments and Financial Intermediation, all of the General Conditions for Current Deposit, in particular as a result of any irregularity in the process of transmission and/or authorisation of the said order that is not duly remedied within 72 hours.

4. Once authorised and sent to the Bank for immediate processing, no amendments may be made to or cancellation of orders transmitted by means of remote communication channels, without prejudice to the provisions of Chapter B - General Conditions for the Provision of Payment Services of the General Conditions of Current Deposit.

5. Considering that the services and/or operations provided by the Bank through the remote channels shall be subject to interferences, interruptions, disconnections or other anomalies, namely in the event of breakdowns, power surges or other events outside the Bank's control, the Customer expressly accepts that the Bank shall not be liable for current or potential damage or losses, including future earnings, that may directly or indirectly result to the Customer from such events, in the extent that those interferences, interruptions, disconnections or other anomalies have been originated by acts or omissions from third parties, as well as bank's suppliers or services license providers and services held and controlled by them.

6. The "Bank Mail" function of the Internet and Mobile channel does not obligate the Bank to execute the orders, unless this is expressly agreed.

7. Only for the Contact Centre channel, and in the case of Tenants-in-common accounts with no powers of autonomous operation by the Customer, the execution of any operation depends on the Bank's prior receipt of confirmation, in writing, from all account holders who are liable for the account, which must occur within 48 hours of the respective transmission. The Customer accepts that, in these cases, the confirmation is sufficient means of proof for the operations therein mentioned.

8. In the Contact Centre channel, with the correct answer to the questions that are asked to the Customer in each telephone contact, in accordance with the Customer's identification and recognition procedures in force, and the Customer's agreement

to the specific proposals that may be made by the Bank, the Bank is hereby authorized to debit the amount and costs associated with the respective transaction.

9. For safety reasons and as a means of proof, the Customer authorises the Bank to record all conversations under the scope of the personalised telephone channel, recognising the validity of these recordings as full evidence of the will to establish a business relation manifested by any of the parties via that channel, namely information, clarifications, or counselling provided by the Bank, of orders and instructions transmitted by the Customer, or the subscription by the Customer to services marketed by the Bank.

Clause 9. Operations recording

1. The Customer and the Bank agree that the computer recording of operations carried out under this Agreement, which may be viewed on screen and/or printed on paper, constitutes appropriate evidence of the orders given by the Customer.
2. The Bank undertakes to maintain the information it provides to the Customer via the Internet, Mobile and MTM channels permanently updated. However, the Bank's own accounting records shall always take precedence over this.

Clause 10. Suspension, blocking access, contractual alterations, termination and rescission of the Agreement

1. The Bank may inhibit and block, temporarily or permanently, access(s) to the remote communication channels by the Customer and/or any of its facilities or services for objectively justified reasons relating to:
 - (a) Security reasons, namely if the Bank is informed or has knowledge that a breach of confidentiality of the Customer's personalised security code(s) and credentials indicated in clause 6 (Convention on proof) has occurred, namely in the event of loss, theft or misplacement thereof, or suspicion of unauthorised or fraudulent use, or loss or misplacement, loss or theft of a bank card of which the Customer is a Holder;
 - b) The suspicion of unauthorised or fraudulent use, or of any irregularity that may result in serious prejudice to the Bank, the Customer or the Payment System, namely when requested to do so by the Payment System management entity for security reasons or for reasons of abuse, misuse or unauthorised use;
 - c) If the Customer carries out illegal transactions of any nature;
 - d) If the present Agreement ceases, in any way, its effects;
 - e) if the Customer is declared bankrupt or insolvent, or if the balance of the Customer's account(s) is unavailable as a result of a court order for attachment, garnishment, seizure or any other form of judicial seizure or other blocking or similar orders decreed by judicial, legal or supervisory authorities.
2. In the cases referred to in the preceding paragraph 1 of this clause, the Bank shall inform the Customer of the blocking of the access(s) to the remote communication channels by the Customer, and of the justification thereof by SMS to the Customer's mobile phone, if possible before the blocking takes place or at the latest immediately after the blocking, unless such information cannot be provided for objectively justified security reasons or is prohibited by other applicable legal provisions.
3. As soon as the blocking reasons cease to exist, the Bank shall unblock access(es) to the remote communications channels by the Customer.
4. In addition to the cases referred to in the preceding paragraph 1 of this clause, it is understood that for security reasons the Customer will be inhibited from accessing the remote communication channels if there are three consecutive failures in the use of the User Code and/or Multichannel Code. In this case, the reactivation of the User Code and/or Multichannel Code may be obtained through an in person contact at a Bank Branch or by telephone through the Contact Centre channel. If it is not possible to reactivate the original codes, under the terms of the previous number, new codes should be obtained through the means available for that purpose, such as Bank Branches, the www.millenniumbcp.pt website or Multibanco ATMs.
5. This Agreement shall have an indefinite duration.
- 6.1. This Agreement may be terminated without giving rise to any grounds or reasons:
 - a) At any time, by the Customer, by means of a written instruction duly signed by the Customer in person at a Bank Branch;
 - b) By the Bank, in this case, by giving sixty days written notice of the date on which termination shall take effect, sent to the Customer under the terms provided in clause 14 (Additional Provisions) below.
- 6.2. The Agreement termination implies the cancellation of access to the remote communication channels by the Customer.

7. The Bank may, by written communication sent to the Customer in accordance with Clause 14 (Additional Provisions) below, terminate this Agreement with immediate effect, immediately cancelling the Customer's access to the remote communication channels in the following cases:

- a) When bankruptcy, insolvency has been declared, or the Bank has knowledge of the Customer's judicial declaration of major accompaniment;
- b) When the Customer unlawfully revokes payment orders he/she has given using remote communication channels;
- c) When it is found that the Customer, through gross negligence or wilful misconduct, has caused damage to the Bank or any other operator or party involved in payment or credit operations through remote communication channels;
- d) If the balance of any Customer account is unavailable following a court order for attachment, enrolment, seizure or any other form of judicial seizure or other blocking or similar orders decreed by judicial, legal or supervisory authorities.

8. The Contract shall also cease to be in force and the right of access to the remote communication channels shall cease immediately in the event of the Customer's death.

9.1. The Bank can propose changes to the clauses of this Agreement, that they arise from legal requirements or are related to international systems and security rules or when deemed suitable by the Bank.

9.2. Such modification(s) will be communicated to the Customer by written notice sent in accordance with clause 14 (Supplementary Provisions) below not less than sixty days prior to the date of its application.

9.3. It is expressly agreed that, in the subsequent silence of the Customer, he/she is deemed to tacitly accept the change(s) thus proposed by the Bank, unless, prior to the entry into force of such proposal, the Customer notifies the Bank that he/she does not accept them.

9.4. If the Customer disagrees with the proposed modification(s), the Customer may rescind and terminate this Agreement immediately, provided that the Customer informs the Bank by registered post with acknowledgement of receipt or by any other means on which a written record is kept.

10. For preventive and security reasons, the Bank may delete the Customer's User Code if, for a period of more than one (1) year, there are no recorded accesses to the Internet, Mobile or MTM Channel. The Customer may recover the User Code at any branch of the Bank by re-registering on the www.millenniumbcp.pt website or by requesting a new access code.

Clause 11. Under-age Customer holder of a current deposits account, aged 14 or more

1. Concerning the current deposits account held by a Customer who is a minor between the ages of 14 and 17, the respective legal representative(s), considering the natural capacity of the minor due to his/her age, may, at his/her sole discretion, request to the Bank, by means of an express written request, that the minor Customer be assigned a User Code and a Multichannel Code, the Bank being free to accept the assignment of said Codes or not.

2. The Multichannel Code shall allow the under-aged Customer exclusively to verify the information - account balances and debit/credit entries - of the current deposits account. No other operations or transactions will be allowed.

3. The Multichannel Code and User Code are personal and non-transferable and shall be given exclusively to the minor, who shall use them in a careful, reserved and exclusively personal manner, and take all reasonable care and diligence measures to preserve the possession, security and reserved and confidential use at all times of his or her mobile telephone or mobile device, and of his or her mobile telephone number previously provided to the Bank, and shall hold his or her legal representative(s) responsible to the Bank for their proper and responsible use, under the terms set out in these clauses.

Clause 12. Financial information

1. The financial information available through the Internet and Mobile channels, namely prices, indexes, news, studies or other, is provided by the Bank solely for information purposes and is drawn up by third parties which authorize the Bank to disclose it to Customers.

2. In spite of the careful selection made by the Bank concerning its sources of information, errors or omissions may not be detected by it; hence, the Bank cannot guaranty the accuracy of the disclosed information nor be deemed liable for the incorrect use or interpretation of such information.

3. The Customer shall use the disclosed financial information at his/her own account and risk and will be exclusively responsible for the investment decisions made based on such information.

Clause 13. Right to free termination

1. The Customer may, under the terms of Decree-Law no. 95/2006, of May 29, freely terminate this Agreement when it is concluded at a distance, without the need to state a reason and without any claim for compensation or penalty.

2. The period for the exercise of the right to free termination is 14 days, counting from the date of the conclusion of the Distance Contract or the receipt of its terms by the Customer, if later.

3. The exercise of the free termination right must be notified to the Bank, namely through a written statement delivered at a branch of the Bank or sent by registered letter with acknowledgement of receipt addressed to Banco Comercial Português, S.A. (Customer Care Centre), Av. Prof. Dr. Cavaco Silva, Tagus Park, Edf. 3, Piso 0, Ala C, n.º 28, 2740-256 Porto Salvo, or by statement sent in a durable support through the Bank's website www.millenniumbcp.pt or App.

4. The exercise of the free termination right extinguishes the obligations and rights arising from this Agreement, with effect as of the date the same is entered into.

5. The Customer is obliged to return to the Bank any amounts or goods received from it within 30 days commencing on the date of the sending of the free termination notice.

6. In the cases when the Bank received any amounts as payment of services, it must return them to the Customer within 30 days commencing on the date of the sending of the free termination notice, unless the Customer has requested the beginning of the execution of the contract before the end of the term for free termination, in which case the Customer is obliged to pay the Bank the value of the services effectively provided.

7. The non-exercise of the right of free termination in accordance with the provisions of the previous paragraphs implies the respective expiration.

Clause 14 Other Provisions

1. During the duration of the current Contract, the Customer is entitled to receive, upon his/her request, at any time, the terms and conditions of the agreement in force at any given moment, in digital format (electronic file) provided to the e-mail supplied by the Customer or for consultation on the Internet channel of the Bank through access to the account at www.millenniumbcp.pt, in accordance with the requirements set forth herein. As an alternative, if the Customer so wishes, he/she can receive the terms of the Contract in paper, if requested in person at any Branch of the Bank.

2. While this Contract is in effect, the communications made by the Bank to the Customer shall be preferably made by e-mail to the e-mail of the Customer supplied to the Bank and/or, if applicable and if possible, by SMS to the respective mobile phone number or as a last resource, to the postal address supplied to the Bank at any moment, in accordance with the provisions of the following paragraphs of this clause.

3. In case of alteration of the respective e-mail address and/or the mobile phone supplied to the Bank, the Customer is obliged to always and promptly inform the Bank of that alteration and to supply the updated e-mail address and mobile phone number to the Bank for the establishment of contacts and communications with the Bank.

4. It is also herein expressly agreed that it pertains exclusively to the Customer to watch out for the regular consultation and permanent update and good functioning of the respective e-mail address and mobile phone number supplied to the Bank for contacts and communications.

5. This Contract and the communications between the parties shall be made in the Portuguese language.

6. The written communications that the Client intends to address the Bank, within the scope of this Contract, may be sent to the preferred branch chosen by the Client or to the Bank's registered office.

7. The Customer shall bear no costs for contacts initiated by the Bank without prejudice to the price or charges due for the financial service which is engaged following each contact.

8. The payment of all financial products and services and insurances acquired while using the remote channels defined in these General Conditions can be made by debiting any account held or to be held by the Customer with the Bank and in respect of which he/she has autonomous powers for debit transactions.

9. The Bank is subject to the supervision of the European Central Bank, with registered office at Sonnemannstrasse 22, 60314 Frankfurt, Germany and of Banco de Portugal, with registered office at Rua do Comércio, 148 (1100- 150 Lisbon), under the Single Supervisory Mechanism, of the Comissão do Mercado de Valores Mobiliários (Portuguese Stock Market Regulator), with registered office at Rua Laura Alves, no. nr. 4 (1050- 138 Lisbon) and of the Insurance and Pension Funds Supervision Authority, with registered office at Av. da República, no. 76 (1600- 205 Lisbon), under the scope of the specific competences of each Entity.

10.1. The Customer may submit complaints or grievances for actions or omissions by bodies and employees of the Bank to the Ombudsman, who will consider them after the necessary investigations have been conducted, and may issue recommendations to the Bank's Executive Committee. The recommendations of the Ombudsman are binding for the bodies and services, after approval by the above-mentioned Committee. Questions should be submitted in writing to the attention of the Ombudsman, using the address available for that purpose at www.millenniumbcp.pt.

10.2. The Customer may also submit claims to Banco de Portugal. For that purpose it may choose to use the Complaints Book available at the Bank's branches or use the Electronic Complaints Book available at www.livroreclamacoes.pt by following the instructions therein disclosed for that purpose, or access online the Bank Client Portal where the Customer may fill in the complaint form online or print and fill in the said complaint form and send it by post to the address of Banco de Portugal, following the instructions therein disclosed for that purpose.

10.3. Disputes involving amounts equal or under those handled by the lower stage courts may, as an alternative to the competent judicial means, be submitted to the following entities specialised in extra-judicial resolution of disputes: Lisbon Consumer Conflicts Arbitration Centre (www.centroarbitragemlisboa.pt) and the Porto Consumer Information and Arbitration Centre (www.cicap.pt).

10.4. The Customer may choose to file for extra-judicial resolution the disputes regarding products and services subscribed online, using the RLL / ODR platform for online dispute resolution (<https://webgate.ec.europa.eu/odr/main/?event=main.home.show>), created for the European Union under the Regulation (EU) no. 524/2013, of the European Parliament and of the Council, of 21 May 2013

10.5. Please be informed that the Bank has available a service for the reception and extra-judicial handling of any claims that the Customers wish to submit; For that purpose, claims must be made through the Contact Centre channel using the numbers indicated in paragraph a) of no. ° 2 of clause 1 and/or by e-mail sent to centrodeatencaoaocliente@millenniumbcp.pt and/or by mail and, in this specific case, the claim must be sent to Banco Comercial Português S.A., Centro de Atenção ao Cliente, Av. Prof. Dr. Cavaco Silva, Tagus Park, Edf. 3, Piso 0, Ala C in article 12 (28, 2740-256 Porto Salvo).

11. For all matters arising from this contract, the competent courts of law are those of Lisbon, Oporto and of the Client's residence in Portugal, waiving all others.

ANNEX 1 - RISKS AND SAFETY RULES

1. General rules for accessing/using of all the remote communication channels of the Bank

1. The Customer commits to read carefully and strictly comply with the security rules and recommendations stated herein, as well as to consult and read, at least once every three months, the security warnings and the periodical warnings that Banco Comercial Português, S.A. (Bank or Millennium bcp) discloses at its website www.millenniumbcp.pt, including the description of specific frauds attempted at any time for the fraudulent capture of the User's Code, the Multichannel code and remaining customized credentials of the Customers to access the remote channels.

2. The Customer must beware and be prepared against fraud attempts by unauthorized third parties. Namely, the Customer must be suspicious of:

a) the degree of urgency of the messages threatening the Customer with the suspension of access to the account, of access codes or of the payment card if the Customer's data are not supplied immediately;

b) the curiosity created by the message which offers a much desired service or product;

c) the request for confirmation of personal data via e-mail or SMS, namely forwarding the Customer for the filling in of a form for the provision of personal data and access codes;

d) spelling/grammar errors and other errors visible in the message or in the fraudulent web page or other data that suggest the suspicious origin of the same;

e) of e-mail messages or SMS with attached links or files;

e) the indication that the Customer must supply Authentication Code(s) sent by the Bank by SMS or generated via Token for the simulation/cancellation of transactions;

3. Millennium bcp never sends e-mails or SMS with links and never requests confirmation of the Customer's personal data or data to access accounts via these communication means, namely instructing the Customer for the online filling in of personal information forms and supply of access codes and credentials nor requesting the Customer to call a determined phone number. If such happens, the Customer must consider that it may well be a fraud attempt.

4. The Customer should analyse the e-mails received before opening them, always confirming the source and the subject, if possible, with the issuer entity; The Customer should not accept the execution of files/programs the download of which is activated without his/her request.

5. The Customer must never disclose the Authentication Code(s) to third parties under any pretext and commits to make a cautious, prudent and exclusively personal use of the same, assuming all risks and consequences deriving from their undue disclosure.

6. If, at any moment, the Customer verifies that his/her mobile phone is inactive and that the mobile phone number is not functioning properly, the Customer must immediately contact his/her telecommunications operator and ensure the correct functioning of the SIM card linked to his/her mobile phone number supplied to the Bank.

7. If, at any moment, the Customer:

a) Suspects that third parties are aware of his/her Users Code in whole or in part and/or of the User's Code and/or Multichannel code or, in case of loss, misplacement, theft, robbery or abusive appropriation of the same or any of them, and/or

b) Verifies the recording in the account of any non-authorized transaction or the existence of errors and irregularities in the making of transactions, and/or

c) Receives an Authentication Code to simulate/cancel a transaction and/or

d) Receives an Authentication Code to confirm a transaction that the Customer did not request ,and/or

c) Suspects of undue access by third parties to his/her e-mail address and/or his/her mobile phone, computer, or portable device or to his/her mobile phone number by any way whatsoever.

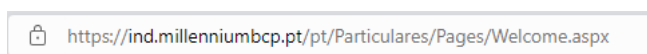
Then, the Customer should suspend the procedure and, without any unjustified delay, contact the Bank by calling +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call), which is a permanent Customer assistance centre - 24/7, 365 days/year, so as to warn the Bank and request the respective locking/prevention of abuse or fraud against it. The cost of communications will depend on the rate you have agreed with your telecommunications operator. The Customer should also confirm what happened before the Bank, in writing and within 5 days.

8. When the Customer wishes to see some security issue approached in our newsletter or requires any clarifications, the Customer must contact the Bank through the e-mail address particulares@millenniumbcp.pt or use the phone number indicated in the previous paragraph.

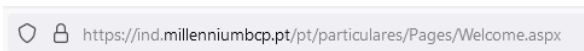
Additional rules to access the internet channel www.millenniumbcp.pt


1. Whenever the Customer accesses his/her bank accounts through the website of Millennium bcp, the Customer should check if the address starts as follows, as per the browser used:


Edge



Firefox

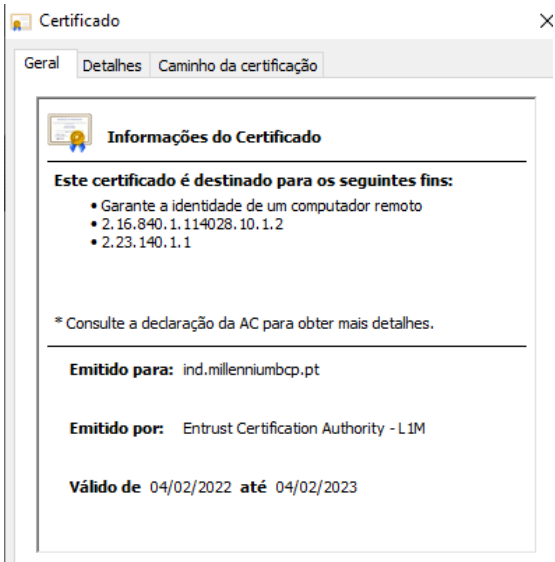


Chrome  ind.millenniumbcp.pt/pt/particulares/Pages/Welcome.aspx

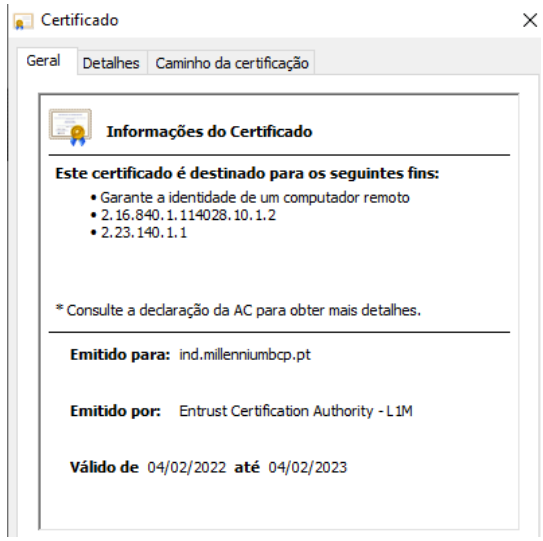
Safari  Millennium BCP(Banco Comercial Português, S.A.) [PT] | ind.millenniumbcp.pt/pt/particulares/Pages/Welcome.aspx

In case of doubt, confirm the origin of the digital certificate - double click on the padlock - and check if it effectively identifies Millennium bcp;

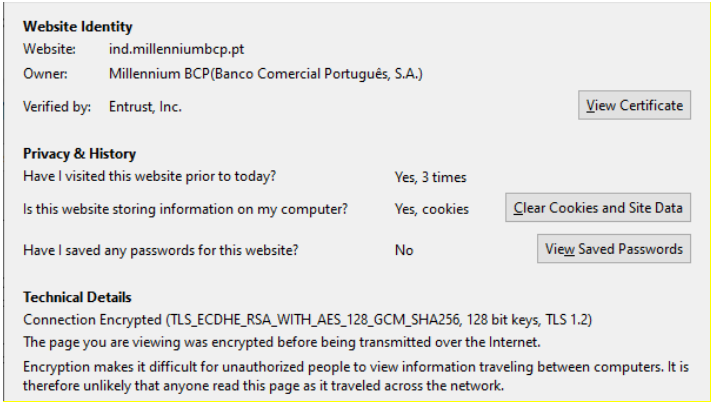
Edge



Chrome



Firefox



Safari



2. In the access to the website www.millenniumbcp.pt the Bank never requests the mobile phone number or the installation of software/security programs.

3. If you are a user exclusively of the website www.millenniumbcp.pt, it will be requested, in the first access and every 90 days, the identification of the User Code, three (3) random digits of the Multichannel Access Code and an Authentication Code generated via Token or sent by SMS to the Client's mobile phone registered at the Bank. In the remaining accesses will only be requested the identification of the User Code and three (3) random positions of the Multichannel Access Code. The same 3 digits will be requested until the login is successfully made. Everything that is requested in addition to what is mentioned above is a fraud attempt that the Customer must immediately report, without any unjustified delay, by calling +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call) a permanent Customer assistance centre - 24/7, 365 days/year, so as to warn the Bank and request the locking/prevention of abuse or fraud against it. The cost of communications will depend on the rate you have agreed with your telecommunications operator.

4. To consult the entries made in the account(s) or bank statements dating 90 days back or more, an Authentication Code will always be requested when, while accessing the website www.millenniumbcp.pt the Authentication Code, generated via Token or sent by SMS to the Client's mobile phone registered at the Bank has not been requested, apart from the three (3) random digits of the Multichannel Access Code.

5. In the making of payment operations by debit of the current deposits account or an account associated with the service, an additional confirmation may be required through (i) a Customer Strong Authentication System (AFC) - in that case, the Customer will be requested to enter an Authentication code generated via Token or sent by SMS to the Customer's mobile phone number registered with the Bank, at the moment the same are carried out.

6. The Customer should carefully read the SMS received containing the Authentication Code since the transaction data are identified in the text message.

7. The Authentication Code will not be requested when making a payment:

- for one of your beneficiaries/favourites previously defined as reliable;
- for accounts held by the Customer with Millennium bcp;
- of a low amount, until it reaches an accumulated amount defined by the Bank.

8. Millennium bcp always sends e-mails and SMS with no links.

9. The Customer should never open Millennium bcp's website through links on messages, search engines or even through the option "Favourites". The Customer should always type in the complete address www.millenniumbcp.pt to avoid accessing untrustworthy pages, very similar to Millennium bcp's website, as well as to avoid the installation of malware in the equipment used to access Millennium bcp's website.

10. Millennium bcp never requests personal and/or confidential data, as for example the entire Multichannel Access Code, mobile phone number, change of data, in the access to the website www.millenniumbcp.pt, by email, SMS or by any other mean.

11. Don't use obvious Multichannel Access Codes (equal numbers, sequential numbers, personal data such as for example the date of birth; mobile number) to access the website www.millenniumbcp.pt. The Customer should periodically, at least every three months, alter his/her multichannel Code in the area "Customize the menu "Área M";

12. Define unique Access Codes for the website www.millenniumbcp.pt and don't use them on other websites.

13. Access to www.millenniumbcp.pt can also be done through the authentication service Digital Mobile key provided by the Portuguese Government.

14. The Digital Mobile Key enables the user to be authenticated through:

- a) Mobile Number;
- b) PIN - Non-transferable personal identification number created when of the registration of the Digital Mobile Key;
- c) The one off and temporary Safety Code formed by 6 numbers sent by SMS to the mobile phone number.

15. By selecting this form of authentication you will be redirected in a safe manner to the Government's authentication service.

being informed of the personal data requested by the Bank and explicitly agrees with that transmission, as per:



16. Never give third parties personal identification data that can be used for certification with the mobile phone operators, or User Codes, Multichannel Access Codes or other codes, namely authorisation codes received by SMS or via Token. The Bank NEVER contacts the Customer to request the Authentication code sent by SMS.

17. The Customer should also prevent third party access to the equipments used to confirm banking operations, as well as to their components, such as the SIM card of the mobile phone number provided to the Bank.

18. The Customer should keep his/her computer protected and should commit, to, namely:

- Install a good anti virus and keep it constantly updated;
- Use a firewall to filter Internet traffic in and out of the computer;
- Pay attention to the security updates that credible software companies provide and install them according to the instructions given.
- Always use updated versions of browsers and operating systems;
- Deactivate the options save the password and browser autofill;
- If the computer is shared with someone else, the Customer should beware and always apply basic protection measures: close the browser window and always end each session and delete the cache memory;
- The Customer should not open e-mails with an unknown origin and especially should not click on or open attachments or links appearing in those messages .
- The Customer should not open files sent by unknown senders;
- The Customer should keep himself/herself up-to-date on general safety concerning the use of internet;
- The Customer must bear in mind that free Wi-Fi networks facilitate access by third parties to his/her mobile phone and to its data and communications. The Customer should not use public Wi-Fi networks to access the website or mobile channel of the Bank nor to access websites requiring the entering of sensitive information, make online purchases and homebanking. For this type of accesses, use always and only your data network;

Additional Rules to access the Contact Centre channel

1. The access to the Contact Centre is made by calling +351 918 27 24 24 / +351 935 22 24 24 / +351 965 99 24 24 or, from abroad +351 210 05 24 24, through VRS (Voice Response System) or personalised servicing being in both cases, requested the Customer's tax identification number and 3 (three) random positions of the Multichannel Code. The cost of communications will depend on the rate you have agreed with your telecommunications operator.

2. To validate a transaction, it is necessary a unique use code generated by Token or sent by SMS to the Customer's mobile phone at the moment the same is made, which will identify the data of the transaction or of the confirmation of the transactions with some random positions of the Multichannel Code. To carry out some transactions or to change personal data, additional security data (personal or related to the Bank) may be requested.

Additional rules of access to Mobile Channel

1- The Customer should:

- a) Activate a form of automatically blocking his/her mobile equipment and of unblocking it by means of a secret code or biometric data of the Customer;
- b) Protect his/her smartphone/tablet with a good antivirus, keeping the same always updated and operational;
- c) Pay attention to the security updates that credible software companies provide and install them according to the instructions given.
- d) Deactivate the option for the installation of apps with unknown origin in the security settings of your equipment;
- e) Always resort to the official Website /stores when needing to install any app and be cautious before making the download of an app, read the opinion from other users and verify which tools and permissions the Customer will have to give access to in his/her equipment (ex: reading and sending of sms, access to contacts, location). It is crucial that the Customer pays attention to the permissions it grants to the apps it installs in its mobile equipment;
- f) When using the e-mail in its mobile device the Customer must certify that it never accesses messages that the Customer does not recognise, mostly attachments or links appearing in those messages. In case the Customer receives any suspicious e-mail allegedly sent by the Bank, the Customer should not open the same and report the fact to the Bank by calling +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call), a permanent Customer assistance centre - 24/7, 365 days/year, so as to warn the Bank. The cost of communications will depend on the rate you have agreed your telecommunications operator.
- g) The Customer must bear in mind that Millennium bcp NEVER sends e-mails and SMS with links;
- h) The Customer must bear in mind that free Wi-Fi networks facilitate access by third parties to his/her mobile phone and to its data and communications. The Customer should not use public Wi-Fi networks to access the website or mobile channel of the Bank nor to access websites requiring the entering of sensitive information, make online purchases and homebanking. For this type of accesses, use always and only the data network of the mobile equipment;
- i) Deactivate the Bluetooth when it does not need it since the mobile phone will be less vulnerable to cyber attacks.
- j) keep your smartphone physically safe and under constant surveillance.

Millennium App

1. The apps of Millennium bcp to be installed and used in mobile phones are available for Apple and Android TM devices.
2. Install the apps through the brand's official web stores (Apple Store and Play Store). Never do so using links provided to you by third parties, namely by e-mail or by SMS.
3. Registration on Millennium App
 - a) After installing the Millennium App, define the unique access code (PIN) composed of 4 numbers, to access Millennium App and do not use it in other Apps;
 - b) Afterwards enter the User Code and three (3) random positions of the Multichannel to validate the sending of the Authentication Code by SMS, indispensable for the registration of the App;
 - c) Lastly, enter the Authentication Code you received by SMS.
4. Access to Millennium App;
 - 4.1. The login to the app is made using a 4 digit PIN code defined during the registry procedure;
 - 4.2. As an alternative to the use of a PIN, you can login to the Millennium APP using fingerprint or facial recognition, if the device provides these technologies. In the login page you will always have the possibility of accessing using the fingerprint, facial recognition or through the PIN. To activate/deactivate access to the Millennium App through Touch ID or Face ID just go to "Settings".
 - 4.3. Don't use an obvious Multichannel Code (e.g. in 1234; 1111; date of birth; postal code) to access the Apps from Millennium bcp. Periodically, alter your PIN using the Profile icon (upper right corner), available after you access Millennium App. Afterwards, select Safety » alter PIN.
 - 4.4. If you consecutively fail three times to enter PIN, you shall have to register again in the Millennium App, as described in 3 above, to define a new PIN.
5. To carry out transactions, the Millennium App may request:
 - three (3) random digits from the Multichannel Access Code; or,
 - An Authentication Code sent by SMS to the mobile phone number registered at the Bank; or,
 - A biometric data (fingerprint or facial recognition).If additional information is requested, it is an attempt to commit fraud and you should report it by calling +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call) a permanent Customer assistance

centre - available 24/7, 365 days/year. The cost of communications will depend on the rate you have agreed with your telecommunications operator.

6. The Authentication Code will not be requested when making a payment:
- for one of your beneficiaries/favourites previously defined as reliable;
 - for accounts held by the Customer with Millennium bcp;
 - of a low amount, until it reaches an accumulated amount defined by the Bank.

Extension of Millennium App to Apple Watch

1. The application for the Apple Watch is an extension of the Millennium App and is activated from it, therefore it requires prior subscription to the above mentioned App in accordance with the terms mentioned above.
2. To use this application you need to set up, in the Millennium App, the accounts/cards you want to view through Apple Watch.
3. The consultation of bank information provided by the Apple Watch application does not require entering a PIN code. However, bank information will only be available when the Apple Watch is near the Customer's iPhone, being this circumstance a security measure that the Customer should always be aware of to safeguard the confidentiality of the information that directly concerns him/her.

Millennium App 'Personal Assistant' Extension

1. The Chatbot is available in the Millennium BCP App and will seek to answer any question or request that the Customer may address to it. Whenever applicable, in a first instance, the user will be redirected to an automatic response flow, where, in self-service mode, he/she can get clarification. Whenever this does not happen, the user may connect by that same channel to the Millennium BCP Contact Centre and, by text, communicate with an assistant who will invest all his efforts in helping him/her.
2. By using the Chatbot extension of the Millennium App, the Customer understands and accepts the fact that the Bank uses subcontracted entities for voice processing and transcription in writing, in the voice case (dictation), and for processing, interpretation and transcription in writing, of the data captured in the image, if using the camera (for data collection).
3. Before executing any order or instruction transmitted through the Chatbot, the Bank will ask the Customer to confirm that it has correctly processed and interpreted the orders or instructions communicated to it.

Additional rules to access MTM

1. The access the MTM is made using a payments card or User Code and three (3) random positions of the Multichannel Code. You will always be requested to enter the same three (3) random positions until accessing is successful; therefore, if additional information is requested (ex: complete Multichannel Code, mobile phone number) it is an attempt to commit fraud and you should report it by calling / +351 918272424 / +351 935222424 / +351 965992424 (domestic call) and +351 210052424 (international call). The cost of communications will depend on the rate you have agreed with your telecommunications operator.
2. Never give personal identification data or user, multichannel or other codes to third parties.

Risks

Failure to comply with the rules and recommendations on the use of remote communication means issued above may lead to the risks for the Customer, namely the following ones:

- Third parties may gain access to personal and confidential data;
- Third parties may execute transactions using the assets in the account and generate financial losses.

ANNEX 2 - OPEN BANKING

1. It is up to the Customer to assess if he/she wishes to share or not his/her banking data. Open Banking affords the client the possibility to share with third parties balances and transactions of accounts held at the Bank but only if the Client gives his/her express consent.

2.1. If the Customer considers suitable that certain institutions or payment service providers, without any contractual connection with the Bank (third parties payment services providers - TPPs) have electronic access to the payment account balance held at the Bank, as well as to other financial information of the account, or start using the account to make payments, the Customer may contract with these institutions or operators some of the following Open Banking services:

- Payment Initiation Services;
- Account Information Services;
- Balance Confirmation Services.

The payment Initiation Services allow for a TPP to set up a payment order in the account which the client holds at the Bank (ex an online payment directly in the client's account to the TPP account).

The information Services on the accounts allow a TPP to gather in its website, financial information from several accounts, including balances and transactions of the account the Client holds at the Bank (financial institutions or entities that run price comparison sites will be among the companies that provide this type of service).

Balance confirmation services allow a TPP issuing card-based payment instruments, at the time the Customer makes a card payment, to confirm that the account held with the Bank has sufficient balance to make the payment.

2.2. The possibility for a TPP to provide the services mentioned above, requires that the account held at the Bank is accessible in the digital channels of the Bank and consequently, the prior subscription by the Customer to the current Agreement for the Use of Remote Communications Channels.

2.3. The Customer's consent for the provision of payment initiation service or account information service or confirmation of balances must be given directly to respective payment initiation or accounts information or balance confirmation service providers. The provision of these services requires that the account is accessible online through the website www.millenniumbcp.pt, that the service provider(s) is/are duly authorized or registered by the competent authorities to provide the respective services, that the same are properly authenticated with the Bank and communicate with it in a safe manner, in accordance with the regulations applicable at any moment.

2.4. For the purposes of the provisions of the previous paragraph, the Customer has the possibility of directly authorising a payment initiation service provider to access information on the account and to give to payment orders to the Bank using the account and/or authorise a payment service provider to access information on the account and respective balances.

2.5. It is expressly agreed herein that the Bank is entitled to provide the information and to execute the payment orders within the scope of the payment initiation services and information on accounts when the respective service providers contact the Bank requesting such information, transmitting such payment orders provided that all the requirements set forth in 2.3 above are complied with and the Bank is successful in obtaining the strong authentication from the Customer.

2.6. The verification of the circumstances foreseen in the precedent number correspond to the express consent by the Customer for the provision of the respective services, in those cases, the Bank should consider any request for information or order or instruction received from the respective service provider as being a request for information, order or instruction given to the Bank by the Customer itself. It is up to the Customer to certify if the service provider that he/she/it uses has his/her/its express authorisation to access the account that he/she/it holds with the Bank, being also responsible for the consequences deriving from supplying customized authentication codes through the remote channels to non-authorised third parties, being also responsible for any consequent losses.

2.7. The Bank is obliged to make the IBAN of the account held by the customer at the bank available to the TPP and, depending on the case, the respective balance or the balance and transactions, or to accept the payment operation initiated by that party, and the TPP does not have to identify the Customer nor to make proof of the contract signed with him/her to provide Open Banking services and have direct access the Bank.

3. It is the Customer's responsibility, once redirected to the Millennium bcp website/app, to confirm the authorisation given to a TPP to provide certain Open Banking services and have direct access to the Bank, and he/she should to that effect, at www.millenniumbcp.pt, correctly introduce the User Code, three random positions of the Multichannel Access Code and an Authentication Code sent by SMS to the phone number registered at the Bank or obtained via Token, or in the Millennium App, to correctly introduce the Security PIN made up of four numbers and an Authentication Code sent by SMS to the phone number registered at the Bank. Therefore, if additional information is requested, it is an attempt to commit fraud and you should report it by calling +351 918272424 / +351 935222424 / +351 965992424 (domestic call). From abroad call +351 210 05 24 24. The cost of communications will depend on the rate you have agreed with your telecommunications operator.

4. The User Code, the Multichannel Access Code and the PIN, indicated in ANNEX 1 - RISKS AND SAFETY RULES of are personal, confidential and not transferable authentication data and therefore the Customer cannot allow their use by third parties, using them in a strict and exclusively personal manner.

5. Before deciding to share with third parties the balances and transactions of the accounts held with the Bank, the Customer must take the necessary steps to confirm that the TPP is a legitimate entity, namely whether it is a registered entity with Banco de Portugal or the competent national authority of the country of origin.

6. It is the TPP's obligation to provide clear and objective information about its identity and contact details, purpose and basis for the processing of information concerning the Client, the recipients of the data if there are any, the fact that it intends to transfer data to a third country, if that is the case.

7. The Customer must take into consideration that if he/she decides to give consent to TPPs to access bank data and if, in addition, confirms in the Millennium bcp website/app the authorisation given to a TPP to provide a certain Open Banking service and have direct access to the Bank, the Bank cannot guarantee the way or the purpose in which that information will be used by him/her, and because it is a payment Initiation Service, the transaction is therefore deemed as authorised, and the consent given for its execution cannot be cancelled. Notwithstanding, after the customer's consent, under the terms mentioned above, and having had access to bank data that concerns it, the TPP is solely responsible for the security of the data thus obtained.

8. The Customer should bear in mind that he/she can manage and cancel the authorisations for Open Banking provision of services given to the TPPs at the website/Millennium bcp app, by accessing the Area M at www.millenniumbcp.pt. The Customer can also call the Millennium bcp Helpline.

9. In any event, in accordance with the law, the Bank has the prerogative to refuse access by a TPP to the Customer's bank data if it considers that there is a risk of fraud