Banque Internationale à Luxembourg
société anonyme
69, route d'Esch · L-2953 Luxembourg · Tél.: (+352) 4590-5000
R.C.S. Luxembourg B-6307 · BIC Code : BILLLULL
TVA : LU 11180925 · LEI Code : 9CZ7TVMR36CYD5TZBS50

NEW DEBIT CARD GENERAL TERMS AND CONDITIONS

1. Description of service

The Visa Debit card (hereinafter referred to as "the card") offers the option to carry out certain banking transactions in Luxembourg and abroad from an automatic teller machine (ATM) or pay for purchases at electronic payment terminals (EPTs) including e-commerce transactions. The card can also be used to make cash deposits in the Bank's Servibank+ network. The conditions of use for the available operations are defined under section 3.

ATMs and EPTs can be accessed by inserting the card in the device and entering a confidential PIN on the keyboard. The card sent is inactive; this act of entering your PIN will activate it. The cardholder may also carry out payments on EPTs offering Near Field Communication (NFC) functionality without needing to insert the card, i.e. without that card coming into physical contact with the terminal and without having to enter his PIN; depending on the transaction amount or the number of NFC transactions carried out, the user may be required to enter the card and/or PIN. The NFC function is activated when the first transaction is carried out in online mode by inserting the card in the EPT or ATM and entering the PIN. The account holder may request from the Bank the deactivation and subsequently the reactivation of the NFC feature. Deactivation of the NFC function is only effective for the card in circulation. If the card is renewed or replaced, a new request must be made to the Bank.

The Bank will send the PIN and the card by post, under separate cover, to the address they have specified.

The card is in the holder's name only and is not transferrable.

On receiving a new card as a replacement for a previously held card, the holder promises to destroy the old card.

The use of the personal and secret number and the use of the card by means of NFC technology have the same binding force on the account holder and on the cardholder and have the same validity as a handwritten signature.

This card is the property of the Bank. The card must be returned to the Bank at the end of this agreement and in any case before the account to which the card is linked is closed; the account statement only becomes final after all transactions have been recorded.

Cash withdrawals and other permitted operations will be debited direct to the account and are equivalent to cash transactions They are usually booked to the account within 10 business days following the date of the transaction, if carried out in Luxembourg. Deposits are immediately credited to the account chosen by the holder except when the network is under technical maintenance. The Bank must immediately be notified of any account entry made for an unauthorised transaction, any error or other irregularity in the management of the account. The Bank may not be made liable for the non-functioning of automatic teller machines and/or electronic points of sale if such malfunctioning is notified by means of a message on the machine or by any other visible means.

The Bank may issue cards to agents at the account holder's request.

The card is valid until the end of the calendar month and year indicated on it. On expiry, the card must be returned to the Bank.

If this condition is not complied with, the account holder shall be held liable for any consequences that may arise. Unless the holder notifies the bank otherwise two months prior to the expiry of the card, the card will be renewed automatically on the expiry date. A card issued to a child aged under 12 that can only be used to make deposits shall not be renewed on expiry after the holder's 12th birthday.

The card is issued subject to a monthly fee as defined in the Bank's fee schedule, which may be modified pursuant to the General Terms and Conditions of the Bank. The fee is automatically debited from the account. The card may be issued as part of a package, in which case the abovementioned annual fee will be included in the price of the package. The Bank's fee schedule applies in case of replacement of a lost or stolen card.

The card is issued and supplied on the instructions of the account holder.

The account holder is liable for the transactions conducted by the Bank covered by the VISA debit card even if a power of attorney has been revoked.

The account holder and, where applicable, the card holder authorise(s) the Bank to provide third parties (such as companies that manufacture or emboss cards, or technical agents that operate payment systems) with their personal data and accept the Bank's recourse to these third parties in Luxembourg or abroad.

2. Security rules

In order to prevent any abuse of the systems, the card holder undertakes to keep their card safely and not to divulge their personal identification number. The PIN must not be noted on the card or on any other document kept with it.

Failure to observe these security guidelines will be considered as serious negligence and will result in the card holder and accountholder being obliged to bear the entire loss resulting from the misuse of the card, even after the notification thereof as described hereafter.

If the card is lost or stolen or if the PIN is discovered by a third party and if the card is misused, the card holder must immediately notify the Bank's card loss centre (service central de mise en opposition) which operates a 24-hour service by telephoning +352 49 10 10 so that measures to prevent the misuse of the card can be taken as quickly as possible. Telephone conversations may be recorded. These recordings may be used in legal proceedings and shall have the same probative value as a written document. Alternatively, they can block their card on BILnet. The holder is also obliged to report the loss or theft of their card to the local police. The police report must be submitted to the Bank. Except in the case of serious negligence or fraud on the part of the card holder or if the card is used for professional or commercial purposes, the card holder and accountholder will bear the consequences of the loss, theft or misuse of the card by a third party up to the moment of notification referred to above only up to an amount of fifty euro (EUR 50).

The Bank reserves the right to block the card for objective reasons relating to security, for example in the case of suspected unauthorised or fraudulent use of the card. The Bank shall inform the card holder before or immediately after blocking the card.

3. Operations

The card holder may not cancel an order given using their card. The account holder authorises the Bank to debit their account with the amounts of withdrawals, payments at electronic points of sale, transfers made using the card, including any related fees; proof of the operation and its proper execution is provided by the records made by the automatic teller machines/EPTs. The fees linked to these operations are defined in the Bank's fee schedule.

Transactions in foreign currencies are converted into euro by the organisation responsible for international clearing of the various card systems at the exchange rate applied by Visa on the day the transaction is processed, with such amount increased by this organisation's and the Bank's foreign exchange charges (2.09%). The cardholder may ask the Bank for the current exchange rate, it being understood that the exchange rate may vary between the time of asking and execution of the payment.

3.1. ATM withdrawals

Until further notice, withdrawals are currently limited to the amount defined per card and for a period of seven calendar days, it being understood that withdrawals can only be made within the limits of the account balance or an existing credit line.

3.2. Payments on EPTs and e-commerce

Until further notice, payments are currently limited to the amounts specified above, per card and for a period of seven calendar days, it being understood that withdrawals can only be made within the limits of the account balance or an existing credit line.

3.3. Deposits in the Servibank+ network

Whenever the card is used to make a deposit, the holder must choose the account to be credited after entering his secret PIN code. Deposits are limited to EUR 10,000 with a maximum of 200 banknotes (every denomination is accepted). The Servibank+ ATM's records shall serve as proof of the transaction and of the instruction of the holder. The transaction slip printed by the machine is for the holder's personal information only.

3.4. Third-party payment applications

(1) The Bank enables the holder to link their card to certain third-party payment applications by means of which they can initiate payment transactions linked to that card. By activating this service, the holder consents to the provision of the data necessary to provide the service to the payment app publisher by the Bank, and to display transactions made using the publisher's mobile payment service within the application. The cardholder also agrees to receive notifications on his/her phone related to the use of the service. Specific transaction limits may apply. The holder must, where applicable, accept the terms of use and personal data protection policy of the publisher of the application in question. The card holder assumes all liability when accessing this application. The Bank is not a party to the contract between the holder and the publisher of the payment application in question.

(2) The obligations and liabilities of the holder described in article 2 of these terms and conditions, particularly with regard to security, confidentiality and changes in the event of loss, theft or any risk of fraudulent use of the card or PIN, shall apply to the holder in full during their use of any third-party payment application. In this context, the meaning of the term "card" used in these General Terms and Conditions shall also include the device equipped with the

BILL.EN.2024.12

third-party payment application; including, as applicable, the mobile device of the holder. The meaning of the term "PIN" shall include the security mechanism or mechanisms used by the third-party payment application and/or the device on which this application is installed.

4. Term and termination

This agreement is entered into for an indefinite period, except where the agreement is concluded for a card issued to a child aged under 12 that can only be used to make deposits; in which case, the agreement shall not be renewed on expiry of the card after the holder's 12th birthday.

The accountholder may terminate the agreement by sending a registered letter or by handing in a written declaration at a branch office of the Bank. He or she must cut the card in two and return it to the Bank. The agreement shall be terminated only when the accountholder has returned the card to the Bank.

The Bank may terminate the agreement by giving the accountholder two months' written notice.

5. Changes to the terms and conditions

The Bank may amend these General Terms and Conditions at any time by informing the holder no later than two months in advance by post, in an account statement or by any other durable medium. The Bank shall consider these changes approved if it has received no written objection from the holder before the changes take effect. If the holder does not agree with these changes, they shall be entitled to terminate this agreement in writing, free of charge, with effect at any time prior to the date when the change is due to take effect.

Except where stated otherwise herein, the Bank's General Terms and Conditions shall apply. The holder may obtain a copy of the present agreement at any time upon request.

6. Applicable law - juridiction

The relations between the Bank and the holder(s) are governed by Luxembourg law.

The courts of the Grand Duchy of Luxembourg shall have sole jurisdiction to rule over any disputes between the Bank and the holder. The issuer may initiate proceedings in any other court which, save for election of the former as the place of jurisdiction, would normally exercise jurisdiction over the holder.

7. 3D Secure

Purpose

3D Secure is an internationally recognised standard of cardholder identification for online debit card payments and is called "Visa Secure". Its purpose is to enhance online transaction security. The cardholder may check whether the retailer has chosen to secure payments using the 3D Secure standard directly on the retailer's website. These Terms and Conditions set out the provisions for the use of 3D Secure technology. They supplement and form part of the general terms and conditions of the issuer relating to the use of Visa cards (hereinafter the "General Terms and Conditions of Card Use") and governing the relationship between the bank (hereinafter the "issuer") that issued the debit card (hereinafter the "Card") and the cardholder and/or user of the Card (hereinafter the "cardholder").

Activating 3D secure for a card

(1) The bank reserves the right to automatically activate 3D Secure for cardholders. Based on the information at its disposal (LuxTrust certificate), the bank will activate this means of authentication enabling the cardholder to perform online transactions requiring 3D Secure identification (hereinafter "3D Secure transactions"), namely authentication through a LuxTrust Signing Server certificate (Token or LuxTrust Mobile). The cardholder can check whether 3D Secure technology has been activated for their card on BILnet. If not, they may activate it on BILnet. In order to link the LuxTrust certificate to their Card, the cardholder must, when following the activation procedure, enter their LuxTrust User ID and password as well as the One-Time Password displayed on their LuxTrust Token, or confirm the activation using LuxTrust Mobile.

(2) Moreover, the cardholder may set a personal security message. This personal security message will appear during all future 3D Secure transactions.

(3) 3D Secure activation is free and takes place over an encrypted internet connection.

(4) Where applicable, the cardholder must complete the activation procedure for each of their Cards. If the cardholder receives a new Card with a new PIN code (e.g. if their Card is lost or stolen), this new Card must also be activated.

(5) If the 3D Secure activation process is not followed, transactions with online retailers requiring 3D Secure identification may not be executed.

(6) The cardholder may change their 3D Secure means of authentication on BILnet.

Card use and authorisation (Execution of a 3D Secure transaction)

The cardholder must validate the execution of the 3D Secure transaction by using their personal codes (LuxTrust username, password, one-time password, biometric authentication). Entering the requisite security information confirms approval of the card payment in accordance with the issuer's General Terms and Conditions of Card Use.

Obligation of due diligence

(1) The cardholder must ensure that the security information and any device or tool (debit card, LuxTrust certificate) required to validate transactions are stored safely and confidentially. In particular, they must not note down or save their security information electronically, either in full or altered form, whether encrypted or unencrypted, or share it with third parties. The cardholder may set a personal security message when activating 3D Secure on the Card. In particular, they undertake not to note down or save their personal security message electronically, either in full or in altered form, whether encrypted or unencrypted, near to the Card or elsewhere. The cardholder also undertakes not to share their personal security message with a third party or to make it accessible to a third party in any way.

(2) When validating the transaction using 3D Secure, the cardholder must ensure that the following security features are visible in the dedicated portal:

– the web address of the portal starts with "https",

– the padlock symbol appears in the portal's address bar,

– the portal displays the personal security message set by the cardholder (where applicable),

– the portal displays the "Visa Secure" logo. Should one of these security features be missing from the dedicated portal, the cardholder must refrain from validating the transaction. They alone are responsible for any damage that may result from their security information being entered and or a transaction potentially being validated.

(3) Should one of these security features be missing from the dedicated portal or if there is any suspicion that the cardholder's security information is being used fraudulently, the latter must inform the issuer immediately and block the Card in accordance with the provisions outlined in the issuer's General Terms and Conditions of Card Use.

(4) The cardholder must immediately change their personal security message, where applicable, if they have reason to believe that a third party has knowledge of it.

Responsability

(1) The liability provisions specified in the General Terms and Conditions of Card Use and in the General Terms and Conditions of the issuer still apply when using 3D Secure. The issuer does not guarantee that the 3D Secure service will always be available and is not liable for any damages resulting from disruption, interruptions (including necessary system maintenance) or overloading of the systems of the Issuer or of any of the Issuer's appointed third parties.

(2) The issuer shall not be held liable for any failure of the 3D Secure service or for any damages resulting from disruption, poor functioning or interruption to the electronic communication networks (internet and mobile telephony) or public servers, a social conflict or other events outside its control.

8. Processing of personal data

The Bank, acting as a data controller, carries out a processing of personal data, in accordance with Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the "GDPR").

The purpose of the processing is to provide clients with a debit card and to handle the lifecycle of a card (its use, cancellation, replacement, management of the PIN) by collecting the following categories of personal data:

- Identification data (first name, last name, date of birth, place of birth, signature, aso…);
- Contact details (postal address, email address, phone number (landline and or mobile));
- Account data (card number, IBAN);

- Authentication (PIN);
- Transactional data (payments issued with the card);
- Electronic communications (exchanges of electronic communications with the Bank).

The lawfulness of the processing is based on article 6 paragraph 1 (b) of the GDPR, insomuch as it is necessary to the performance of these GTC. Not providing the aforementioned personal data shall make the Bank unable to provide the service to the client.

The recipients of the personal data are the Bank and Worldline Financial Services, both located in Luxembourg. To ensure the functioning of the card within the network, as well as the prevention, detection and analysis of fraudulent transactions, the cardholder and the account holder authorise the Bank and Worldline Financial Services to transmit to third parties, in particular Visalux S.C., all banks and all merchants participating in the international Visa network, all merchants participating in domestic and foreign networks of payment terminals (POS), card manufacturers, as well as the companies that manage card-related insurance, the personal data concerning the card and account holder(s), insofar as the provision of this data is essential for the processing.

The recipients of these personal data may be located outside the European Economic Area and notably in countries where the level of personal data protection is likely to be lower than that provided in the European Economic Area.

In addition to the provisions on the processing of personal data provided for in these General Terms and Conditions of Card Use, the cardholder specifically authorises the Bank to transfer their personal data to third parties whose involvement is required as part of 3D Secure. These third parties include companies responsible for managing the dedicated portal and the codes required to activate the 3D Secure service and validate 3D Secure transactions.

In this context, the cardholder expressly acknowledges having been informed that 3D Secure requires the involvement of third companies for LuxTrust certificate validation and management of the dedicated portal. The transferred data is also likely to be stored by these third companies, including abroad.

In accordance with the applicable legislation, the Bank shall store the client's personal data for a 10-year period after termination of all business relationships with the client.

The client has the following rights regarding the personal data that the Bank processes about him/her:

- Right to access his/her data;
- Right to rectify his/her data;
- Where applicable, right to erase his/her data;
- Right to restriction to the processing of his/her data;
- Right to portability of his/her data;
- Right to object to the processing.

The information requests on the processing and the exercises of rights must be submitted by the client through one of the following channels:

- On the bil.com website, in the "Data Protection" section;
- By email to the dpo@bil.com address;
- By mail to the following address: Banque Internationale à Luxembourg, Data Protection department, 69 route d'Esch, L-2953 Luxembourg.

In case of unsatisfactory answer, the client can also lodge a complaint to the Commission Nationale pour la Protection des Données, located 15 boulevard du Jazz, L-4370 Belvaux.