

# APPENDIX: TERMS AND CONDITIONS OF USE FOR 3D SECURE

## Purpose:

3D Secure is an internationally recognised standard for identifying the holder of a debit or credit card for online payments that use "Mastercard® SecureCode™" for Mastercard® payments and "VERIFIED by VISA" for Visa payments. It is designed to make online transactions more secure. Card holders can check if an online seller has chosen to secure online purchases using the 3D Secure standard directly on the seller's website.

These Terms and Conditions define the terms of use for the new version of the 3D Secure technology. They supplement and form an integral part of the issuing bank's general terms and conditions regarding the use of Visa or Mastercard cards (hereinafter the "General Terms and Conditions for Use of Cards") between the bank (hereinafter "the Issuing Bank") that issued the credit or debit card (hereinafter the "Card") and the holder and/or user of the card (hereinafter the "Client").

### Art. 1: Activation of 3D Secure for a Card

- (1) The Bank reserves the right to automatically activate the 3D Secure technology for eligible Client cards.
- (2) If 3D Secure is not activated, a transaction with an online seller requiring 3D Secure identification cannot be carried out.

### Art. 2 : Utilisation de la Carte et autorisation

- a) Execution of a 3D Secure transaction via a LuxTrust certificate in Token form (hereinafter "the LuxTrust certificate"):

In this case, the Client must confirm the 3D Secure transaction using their LuxTrust username, LuxTrust password and the one-time password provided on their LuxTrust certificate.

- b) Execution of a 3D Secure transaction using LuxTrust Mobile:

In this case, the Client must confirm the 3D Secure transaction using the LuxTrust Mobile application installed on their smartphone and activated following the relevant procedure. The Client will be asked to confirm the transaction in the application by entering the LuxTrust Mobile password or, if applicable, using biometric data.

Entering the required security information confirms that the card payment has been approved in accordance with the provisions of the Issuing Bank's General Terms and Conditions for Use of Cards.

### Art. 3: Duty of care

- (1) The Client must ensure the security and confidentiality of their security information and of any item or device (credit or debit card, LuxTrust certificate) required to confirm the transaction.

As such, they must not note down or save security information in electronic format in complete or modified form, encrypted or otherwise, or disclose such information to a third party.

- (2) When confirming the 3D Secure transaction, the Client must ensure that the dedicated web portal includes the following security features:

- the web portal address must begin with "https",
- the portal address bar should display a padlock,
- the portal should include the "Mastercard® SecureCode™" or "VERIFIED by VISA" logo,
- the LuxTrust secret image chosen by the Client should be visible if they opt to confirm the transaction using the LuxTrust token,
- the transaction details, which appear on the secret image or on the LuxTrust Mobile application, must be visible. These details include the transaction information the Client wishes to confirm.

If one of these security features cannot be found on the dedicated web portal, the Client must not confirm the transaction, and shall be solely responsible for any damage that may result from the use of their security information and potential confirmation of the transaction.

- (3) If one of these security features cannot be found on the dedicated web portal, or if the Client suspects fraudulent use of their security information, they must immediately inform the Issuing Bank and block the Card in accordance with the provisions set out in the Issuing Bank's General Terms and Conditions for Use of Cards.

### Art. 4: Processing of personal data

- (1) The Client authorises the Issuing Bank to process their personal data in order to ensure the proper functioning of the Card and to prevent, detect and analyse fraudulent transactions.
- (2) In addition to provisions relating to the processing of personal data set out in the Issuing Bank's General Terms and Conditions for Use of Cards, the Client specifically authorises the Issuing Bank to disclose their personal data to third parties whose involvement is required for 3D Secure.

As such, the Client expressly acknowledges that they have been informed that 3D Secure requires the involvement of third-party companies to confirm transactions using a LuxTrust certificate. The data disclosed may also be stored by these third-party companies, including abroad.

- (3) As the data controller for the personal data, the Issuing Bank undertakes to process the data in accordance with applicable legislation on the protection of individuals with regard to the processing of personal data.
- (4) The client has the right to refuse the transmission of information within the 3D Secure scope by contacting our Client Service.

### Art. 5: Liability

- (1) The liability clauses in the General Terms and Conditions for Use of Cards and in the Issuing Bank's General Terms and Conditions shall apply to the use of 3D Secure.



**BGL**  
**BNP PARIBAS**

The Issuing Bank does not guarantee the systematic availability of the 3D Secure service, and shall not be held liable for any damage resulting from a malfunction, interruption (including required maintenance) or overload of the systems of the Issuing Bank or of one of the third parties mandated by the Issuing Bank.

(2) The Issuing Bank shall not be held liable for any failure of the 3D Secure technology, including any damage, resulting from a breakdown, malfunction or interruption of electronic communications networks (internet, mobile telephony) and public servers, civil unrest or other events beyond its control.