

GENERAL TERMS OF USE OF THE SERVICE 3-D Secure

Please read the Terms of Use of the Service carefully before using 3-D Secure.

I. Definitions

The individual terms used in the Terms of Use have the following meanings:

- (1) **The Issuer** of the Terms of Use of the Service 3-D Secure (hereinafter: Terms of Use) is the UniCredit Banka Slovenija d.d., Ameriška ulica 2, 1000 Ljubljana, Slovenia, SWIFT (BIC) code BACXS122, info@unicreditgroup.si, registered with the District Court of Ljubljana under registry entry number 1/10521/00, registration number 5446546 (hereinafter: the bank). The bank is listed in the list of banks and savings banks, authorised by Banka Slovenije to provide payment services, and published on Banka Slovenije's website;
 - (2) **The bank website** is the www.unicreditbank.si;
 - (3) **The Cardholder** is the transaction account user, or the person authorised by the user to use the card;
 - (4) **The 3-D Secure** is a service, which enhances the safety of online purchases with the cards Mastercard at points of sale labelled with Mastercard ID Check. The bank uses strong customer authentication or requires that the elements of two-factor authentication are used, confirming the identity of the user by validating online purchases in a mobile bank using biometric data or a PIN code;
 - (5) **The Security Code** is the three-digit number written on the sign strip on the back of the card (CVC code for Mastercard);
 - (6) **The Code** is intended for online payment at points-of-sale with the label Mastercard ID Check;
 - (7) **The 3-D Secure User** is the cardholder, who makes an online purchase at the Mastercard ID Check point-of-sale using a mobile bank and confirming the online purchase using biometric data (e.g. fingerprint or facial recognition) or a PIN code;
 - (8) **The Authentication** is a procedure enabling the bank to verify the identity of the user or the eligibility of the use of a particular payment instrument, including the use of the user's personal security features;
 - (9) **The Strong Customer Authentication of clients** is authentication using two or more elements that fall under the category of user knowledge (something only the user knows), user ownership (something that is in the exclusive ownership of the user) and inseparable connection to the user (something the user is), which are independent of each other, meaning that the infringement of one element does not impede the reliability of the others, and which are designed to protect the confidentiality of the data being verified;
 - (10) **The Biometrics** or biometric validation of online purchases is to confirm the authenticity of the transaction with fingerprint, face, voice, or corneal scanning. The bank is not the controller of biometric personal data; these are stored in the 3-D Secure user's device, if the user of the service allows the device to process such data.
- (3) All information about the rights of individuals relating to the processing of personal data and contact details are set out in more detail in the General Information on the Processing of Personal Data. The currently applicable General Information on the Processing of Personal Data is available at the bank's premises and on its website (www.unicreditbank.si/gdpr).
 - (4) The user and cardholder undertakes to report to the bank any change of the mobile phone contact number for the authentication of the online purchases.
 - (5) The user and cardholder agrees that the bank periodically checks the user and cardholder's data with a view to determine, for the purposes of the Foreign Accounts Tax Compliance Act (FATCA), whether there may be circumstances (U.S. Indicia) that could cause the user and cardholder to be regarded as an American taxable person (U.S. Person).
 - (6) Notwithstanding the above provision, the user and cardholder undertakes to notify the bank in writing without delay of any change in the circumstances of their status (U.S. Indicia), such as obtaining U.S. citizenship, obtaining a U.S. address, obtaining a phone number in the United States, etc. The user and cardholder undertake to inform the bank and provide the relevant documentation demonstrating any changed circumstances.
 - (7) If the user and cardholder does not inform and provide the relevant documents, which show the status of the user and cardholder to the bank immediately upon receipt of the written request from the bank, the bank will inform the tax authority of the Republic of Slovenia that the user and cardholder is a potential American taxable person (U.S. Person). In this case, the bank is entitled to unilaterally terminating the contractual relationship after prior written notification to the user and cardholder and closing the account in accordance with the terms of the Terms and Conditions.
 - (8) The user and cardholder undertakes to reimburse the bank for any costs and damages that may arise as a result of a breach of this Article by the user and cardholder.
 - (9) The bank and the user and cardholder are unanimous that the user and cardholder, by signing the contract in accordance with Article 2(215) of the Banking Act, gives consent that for the purposes of the FATCA the bank can communicate to the tax authority of the Republic of Slovenia individual confidential information about the user and cardholder.

II. General

- (1) With these Terms of Use, the bank governs the protection of personal data and confidential information, the means of use and characteristics of the service, the liability of the service user, the exclusion of bank, Mastercard liability, the notification of the service, the termination of the right to use the service, the transitional and final provisions and the validity of these Terms of Use.

III. Protection of personal data and confidential information

- (1) The bank is the controller of personal and other confidential user data, which are acquired in establishing the business relationship and continuing to do business with the user.
- (2) For the purpose of implementing the mutual contractual relationship, for the purpose of implementing legal requirements, on the basis of

legitimate interest and for marketing purposes to the extent consistent with consent to the processing of personal data, the Bank processes, stores, transmits and protects personal and other confidential data in accordance with the Law Governing the Protection of Personal Data, the General Data Protection Regulation (Regulation (EU) 2016/679-GDPR), the Law Governing Banking, the Law Governing Companies and other regulations relating to the protection of personal and confidential data and trade secrets, and in accordance with their internal acts.

- (3) All information about the rights of individuals relating to the processing of personal data and contact details are set out in more detail in the General Information on the Processing of Personal Data. The currently applicable General Information on the Processing of Personal Data is available at the bank's premises and on its website (www.unicreditbank.si/gdpr).
- (4) The user and cardholder undertakes to report to the bank any change of the mobile phone contact number for the authentication of the online purchases.
- (5) The user and cardholder agrees that the bank periodically checks the user and cardholder's data with a view to determine, for the purposes of the Foreign Accounts Tax Compliance Act (FATCA), whether there may be circumstances (U.S. Indicia) that could cause the user and cardholder to be regarded as an American taxable person (U.S. Person).
- (6) Notwithstanding the above provision, the user and cardholder undertakes to notify the bank in writing without delay of any change in the circumstances of their status (U.S. Indicia), such as obtaining U.S. citizenship, obtaining a U.S. address, obtaining a phone number in the United States, etc. The user and cardholder undertake to inform the bank and provide the relevant documentation demonstrating any changed circumstances.
- (7) If the user and cardholder does not inform and provide the relevant documents, which show the status of the user and cardholder to the bank immediately upon receipt of the written request from the bank, the bank will inform the tax authority of the Republic of Slovenia that the user and cardholder is a potential American taxable person (U.S. Person). In this case, the bank is entitled to unilaterally terminating the contractual relationship after prior written notification to the user and cardholder and closing the account in accordance with the terms of the Terms and Conditions.
- (8) The user and cardholder undertakes to reimburse the bank for any costs and damages that may arise as a result of a breach of this Article by the user and cardholder.
- (9) The bank and the user and cardholder are unanimous that the user and cardholder, by signing the contract in accordance with Article 2(215) of the Banking Act, gives consent that for the purposes of the FATCA the bank can communicate to the tax authority of the Republic of Slovenia individual confidential information about the user and cardholder.

IV. 3-D Secure Usage and Features

- (1) This service provides greater security for online purchases to the cardholder by reducing the chances of scams in transactions.
- (2) The cardholder can use the 3-D Secure service and strong customer authentication, if the following requirements and conditions are met:
 - the cardholder holds a Mastercard;
 - the cardholder is a mobile bank user;
 - the bank has their mobile phone number;
 - the cardholder accepts these Terms of Use of the Service.

V. Process of using the service

- (1) The cardholder makes an online purchase at a point-of-sale that uses a 3-D Secure service or is marked with MasterCard ID Check.
- (2) The cardholder uses a mobile bank to confirm an online purchase at such a point-of-sale, they authenticate and validate the online purchase

by using a PIN code or biometric data after receiving a mobile bank push message, if supported by the mobile device, to confirm or reject an online payment. In case of confirmation of online payment, the purchase is completed.

- (3) The use of the mobile bank is mandatory for a cardholder, who makes an online purchase at a point-of-sale using the 3-D Secure service.
- (4) If the cardholder wishes to change the mobile phone number, this can be done using the appropriate form (in the online bank (Online banka or BusinessNet), or in person at the bank's business unit,...).

VI. Responsibility of the 3-D Secure User

- (1) The user of the Service understands and agrees that Mastercard and/or the bank may change, suspend or terminate at any time the Service or the use of any of the safety components presented, or any part of it, upon prior notice.
- (2) The user of the service understands and agrees that they are solely responsible for ensuring the confidentiality of the verification information, which is transmitted to the bank for the purpose of using the service.
- (3) The user of the service undertakes not to disclose the use nor access to the use of the security feature or mobile device or application through which the two-factor authentication and validation of online payments are carried out nor to allow the use to third parties, but shall access the service and use it only by themselves.
- (4) The user of the service is responsible for ensuring the security and confidentiality of the mobile device on which they use the mobile application. The user of the service is obliged to keep it safe to prevent its theft and/or loss.
- (5) The user of the service undertakes to inform the bank immediately of any unauthorized use of the mobile device or application or access to the use of a security element or any other security breach.
- (6) The user of the service understands and agrees that unless the applicable law provides for otherwise, neither Mastercard nor the bank shall be liable for any loss or damage resulting from their non-compliance with these Terms of Use.
- (7) The user of the service understands and agrees that the service does not imply that the bank or Mastercard recommend or support any supplier that uses the service, and that the service does not verify the identity of the supplier or the quality of the supplier.
- (8) The user of the service understands and agrees that dealing with the supplier or participating in their promotions is exclusively in the domain of the service user and the supplier. The user of the service understands and agrees that neither Mastercard nor the bank are liable for any loss or damage resulting from such business.
- (9) The service user undertakes not to do the following:
 - uploading, publishing, sending by e-mail or otherwise transmitting material containing computer viruses, other codes, files or programs, the purpose of which is to interrupt, destroy or limit the functionality of any computer, software, hardware or telecommunications equipment used by the service;
 - sending unwanted electronic mail messages (spam) or unwanted contents to the website or service;
 - modifying, adapting, translating, selling, reverse engineering, dismantling, or degrading any part of this website or service;
 - removing copyright, trademark or other proprietary rights contained in the service;
 - "framing" or "mirroring" any part of the web page or the service without prior written authorization by Mastercard;
 - using any robot, spider or application to find and retrieve information or other manual or automatic devices or procedures for querying, indexing,

data mining or any other reproduction or deceit of the navigation structure or repositioning of a website or service or its contents;

- interfering in any way with or interrupting or violating the service, or interrupting it, or violating these usage rules or any requirements, procedures, policies or regulations regarding the Service or any networks connected to the service;
- intentionally or unintentionally infringing any applicable local, national, national, or international law, regulations, legal guidelines and/or judicial, administrative interpretations, or any rules or requirements of Mastercard or the bank in relation to the use of the service.

VII. Exclusion of bank and Mastercard liability

- (1) The bank and/or Mastercard shall not be liable for any modification, suspension, or termination of the service.
- (2) The bank and/or Mastercard shall not be liable for consequential, incidental, special or indirect losses or other damages, such as damage to the service user's computer or other equipment or any other viruses, which could damage it as a result of the user's access, use or upload of content from this website.

VIII. Notification about the service 3-D Secure

- (1) Service notifications may be sent by the bank to the last known address of the service user. The bank may also inform the user of the service of changes to these use rules or other matters by posting notices on the bank's website, through notifications in the online bank or with links to these notices.

IX. Termination of the right to use the service 3-D Secure

- (1) The bank may suspend or terminate the service with or without any fault of the service user. The bank will notify the service user of the service termination.

X. Transitional and final provisions

- (1) The user of the service agrees that the use of the 3-D Secure service means the user of the service accepting these Terms of Use.
- (2) Unless expressly provided otherwise, all new functionalities that expand or improve the 3-D Secure service are subject to these Terms of Use.
- (3) If the bank or Mastercard change their rules, effecting a change in these Terms of Use, the bank shall inform the service user before the changes take effect by posting a notice on the bank's website.
- (4) If the user of the service does not agree to the changes to the Terms, they may stop using the 3-D Secure Service without notice.
- (5) The applicable terms of use are published on the bank's website.
- (6) These Terms of Use apply from 1st January 2026 onwards.