Electronic conclusion of contracts under a distance selling scheme

- for payment services (payment account management, bank card services) and for the related electronic services provided to retail customers -

Customer Information Document

The purpose of this document is to provide information to the Customers of the Bank regarding Act XXV of 2005 on the Distance Marketing of Consumer Financial Services ('Distance Marketing Act') and, prior to submitting their applications, on the provision of information by the bank related to electronic contracting on the steps of the entire online process and about the additional terms and conditions of e-contracting with reference to Section I. 6 of the Terms and Conditions for Retail Clients.

Pursuant to the customer information document and contractual documentation that may be requested and provided by electronic means via the Customer's personal account ('Customer Account') generated by registering on the application sub-page of the website of UniCredit Bank Hungary Zrt. ('Bank'), a **consolidated framework agreement is concluded** electronically between the Customer and the Bank for the **provision of payment services** within the context of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises ('Credit Institutions Act') **for financial services and specific electronic banking services** of the Customer's choice[1] and/or for **debit cards,** which shall constitute a written contract.

The Bank's **internet banking service [UniCredit eBanking] is automatically linked to** electronic contracting. This service is designed to send and store electronic contracts securely; moreover, all notifications about the provision of the service are stored here. Electronic contracts become legally binding upon having been made available in the Customer's eBanking account.

Under the contract, you will become entitled to the account management service. In case of the debit card, mobile application [UniCredit mBanking] or telephone banking service [UniCredit Telefonbank] selected for your bank account, following the activation of your bank card and the mBanking service, you as an account holder customer ('Customer') will be entitled to dispose over your accounts and request account and other information through these channels.

The e-contracts concluded by the parties and all contractual terms and conditions in effect at the time of the conclusion of the contract (i.e. the General Terms and Conditions, Customer Information Document(s), Terms and Conditions and Lists of Conditions) will be available – with the original, unaltered content – in the Customer's **eBanking account** at any time throughout the term of the contract(s) concluded for the service and throughout the validity period of the eBanking service. Application for the services and contract conclusion do not entail any additional charges due to their electronic nature.

The Bank's other information provision obligations under the Distance Marketing Act are performed, in respect of the payment account, in the context of the information provision obligation stipulated by Act LXXXV of 2009 on the Pursuit of Business of Payment Services (Payment Services Act).

I. Steps of electronic application and contracting

1. Product selection

The Customer obtains information about the terms and conditions of the bank account packages available online on the www.unicreditbank.hu/onlineszamlanyitas website, and selects the financial services and related services that best suit his/her needs by pressing the 'Apply' button.

[1] The optional electronic banking services that may be selected for individual account packages are the following: Telephone banking service [UniCredit Telefonbank], mobile application service [UniCredit mBanking], SMS service [UniCredit SMS service], bank card service.

All terms and conditions of each individual service are available for download on the website.

Upon product selection, the Customer checks on the interface his/her **compliance with the conditions for using** the selected services (i.e. being a Hungarian citizen of or above 18 years of age acting on his/her own behalf, not being a customer of the Bank, not disposing over any UniCredit bank account, and not qualifying as a politically exposed person or being a relative or close associate of such person).

The Customer receives information – both in graphic and descriptive form – about the individual steps of the electronic contracting process, at which point this customer information document will also become available for download. Throughout the online process, the Customer is supported by graphic navigation so that he/she can identify each process step with the assistance of pictograms.

Online application is also supported by the Bank's over-the-phone assistance service offered continuously on the interface.

2. Registration – application Customer Account

The product selection public website navigates the Customer to the **online application registration** page, where the Customer can fill out the registration form for the online application, creating his/her own personal **Customer Account.**

The purpose of the Customer Account is to perform the application process. The application process may be interrupted and continued later on at any time for a maximum of 30 days after the process has been interrupted and saved. In order to return to the process, click on the unique link sent by e-mail to the Customer Account after the process has been saved, provide the registered mobile phone number on the application interface, and enter (up to 3 unsuccessful attempts) the one-off identification code sent to your mobile phone. After the conclusion of the contract, the Customer Account is terminated, and its function is replaced by the eBanking account requested by the Customer.

In the course of the registration process, the Customer is requested to provide the following contact details: mobile phone number, e-mail address and the following personal data: full name, and using the one-time identification code (valid for 2 minutes) sent to the mobile phone number in SMS, the Customer authenticates the data.

Before the finalisation of the registration, the Customer consents to the Bank's processing of his/her data by accepting the **Data Controlling Guidelines** available on the website for download. In the event the Customer withdraws his/her consent to the recording of his/her data during the due-diligence process, the Bank will discontinue the contracting process.

3. Provision of personal data

Following the registration, the Customer shall provide additional personal data: name at birth, mother's maiden name, country of birth, place and date of birth, citizenship; type and number of the document suitable for identification; address or – in the absence thereof – temporary place of residence. Thereafter, in relation to the selected product the Customer will have an option to change some of the data on the interface, such as: name to be printed on the bank card, level of the telephone banking service and the branch selected as the location of any future personal administration.

4. Verification of the data entered, correction of data entry mistakes

According to Sections 2 and 3 the Customer may read back, double-check and edit (correct) the provided contact details and personal data on the application interface.

5. Customer declarations

The Customer fills out the following declarations:

- the **FATCA and CRS** declarations on tax residency required for account opening,
- the Know Your Customer **(KYC) questionnaire** required for establishing the customer relationship.
- The Customer has an option to give voluntary consent to **direct marketing** messages by the Bank and its intermediaries by specifying the channel for such communications (electronic channels, e-mail, text message).

6. Receipt of the Bank's offer, review of draft contracts

The draft contracts for the selected account package and the related services, all relevant general contractual terms (Terms and Conditions, List of Conditions) and the Customer Information Document are made available for review and download in the Customer Account.

At the same time, access is provided on the Customer Account interface to video identification, to the customer information document on the process, to the documents the Customer needs to have ready and to the time slots available for initiating the video call.

7. Customer identification – video call

Customer identification and due diligence under the Anti-Money Laundering Act are performed during the video call initiated at the time slot indicated in Section 6.
The Customer enters the video call interface by clicking on the link. Following a registration step (in which the Customer provides his/her name, e-mail address, mobile phone number, type and number of the identification document and the number of the address card) and a camera and microphone check the video call is launched. After successful entry, the Bank's operator performs the video identification. The Customer makes his/her declaration regarding his/her beneficial owner and politically exposed person status during the video call.
The Bank performs the Customer's real-time video identification as per the Anti-Money Laundering Act with the FaceKom software provided by TechTeamer Kft. (registered office: 1015 Budapest, Szabó Ilonka utca 9., company registration number: Cg. 01-09-962028, tax number: 23362840-2-41) and based on the Bank's Information Document on the User and Technical Conditions for the Video Call Service made available to the Customer on the application interface which, pursuant to Section 2 (1) of MNB Decree No. 26/2020 (VIII. 25.), qualifies as an audited electronic communication equipment with the relevant audit report issued as per Section 5 of the MNB Decree.

8. Signing the contract, effective date and availability of contract

After successful customer identification, the Customer can proceed to the electronic signature page on the Customer Account interface.

The Customer is provided with sufficient time to review the documents to be signed: to that end, the process can be interrupted and saved – for a maximum of 30 days –, and continued by the Customer as required after repeatedly logging on to the site. Repeated login can be performed by clicking on the unique link e-mailed to the Customer and entering the one-time SMS code sent to the previously provided mobile phone number. After completing the review of the documents, the Customer indicates the comprehension and acceptance of each document by checking the appropriate checkbox. Thereafter, the Customer may attach his/her electronic signature to the consolidated account contract by clicking on the 'signature' button and entering the one-time SMS code sent to the mobile phone number previously provided during the process. If the Customer chooses to reject a document, he/she has the opportunity to initiate a consultation for clarification, to make an appointment with any UniCredit branch within the country for further information, or to make a legal declaration in the branch.

The Customer's signature creates, via identified electronic means, a contractual declaration meeting the criteria defined in Section 6:7 (3) that is deemed to be a written declaration and the content of which and the time of signature is certified by the qualified electronic stamp and timestamp of Microsec Zrt., acting in the capacity of trust service provider registered with the National Media and Infocommunications Authority. The trust service is provided to the Bank under the Bank's contract with Microsec Zrt.

The Bank **confirms** the receipt of the Customer's signed contractual declaration via e-mail.

In the Customer's eBanking account, the Bank makes the contract available for download to the Customer – bearing the Bank's official electronic signature – along with its annexes, and also stores the documents in its own systems. The electronic **contract** is deemed delivered to the Customer and **enters into force** on the day on which the contract signed/certified by both parties is uploaded to the eBanking account.

The Bank sends a separate e-mail to the Customer on the binding entry into force of the contract, also attaching the username required for logging on to the eBanking account and sending the primary password in a text message.

This concludes the entire electronic application and contracting process, and the provision and use of the services may commence.

II. Security requirements of the Customer's communication device and its use

During the distance selling process, the Customer may initiate electronic contracting only through his/her own phone number (also assigned to him/her by the service provider).

For Customer identification, for making electronic legal declarations (signing the contract), for the secure use of the equipment/devices used by the Customer in order to take recourse to the Bank's mobile application service (mBanking) (including in particular, but not limited to: smart phone, personal computer (desktop, laptop), tablet, including software and hardware components and e-mail account (hereinafter: Equipment), and for the protection of the Customer's personal data and bank secrets, it is essential to ensure the adequate maintenance of such equipment/devices, the security of the Equipment by continuously meeting the following - including, but not limited to - security requirements: but not exclusively by continuously meeting the following security requirements for which Customer is solely responsible.

In general, the device:

- available only after successful identification of the customer on the device, the data used for identification are regularly changed, not easy to guess (for PIN code – in case of Smartphone / Tablet-, password)
- its components (operating system, firmware, browser, applications) are regularly updated in accordance with the manufacturer's recommendations and are securely set up
- your network connections are securely set up (use appropriate wireless network security procedures (eg encryption and authentication), restrict access to network devices),
- its display is only visible to the customer during the process
- Saving the username and password in the browser is not recommended
- It is recommended to use a password that is at least 8 characters long and contains small and capital letters, numbers, special characters, does not contain a meaningful dictionary word, it is also recommended to use a dedicated password, the customer should avoid reusing the password used in other services, it is recommended to use a secure password store in general

In addition:

For Smartphone / Tablet device:

- the protection mechanisms, authorization system and other subsystems of the operating system on the device have not been modified (root - Android, jailbreak - iOS)
- SMS Preview is not enabled on a locked display
- PIN is not containing easily guessable, not contains e.g. birthdays, repetitive characters like 111111

For desktop / laptop device:

• has licensed, up-to-date malicious code protection (virus protection, anti-malware) - virus scanning runs regularly, and its scope extends to downloaded files, media connected to the device, with modern protection solutions (eg firewall)]

Moreover, the Customer ensures that access to the communication equipment used for Customer identification and for making electronic legal declarations during the distance selling process is strictly limited to the Customer excluding any access by a third party.

Provisions excluding the Bank's liability

The Bank fully excludes its liability for damages arising from the inadequate security settings or inadequate security level of the Device.

The Bank shall not be held liable for damages arising from any technical flaws of the Customer's equipment or from the Customer's failure to establish adequate connection with the Bank due to such flaws.

The Bank shall deem all applications initiated by Customers logged on to the online application interface verifiably with the relevant identification code (mobile phone) and authenticated by the one-time password sent to the Customer's mobile device to have been initiated by the person specified on the application form, and the Bank shall not check the user authorisation of the person using the identification code and the password (mobile phone) or the circumstances of the use. The Bank shall not be liable whatsoever for damages incurred by the Customer or by any other person arising from applications initiated by unauthorised persons using the identification code and the password assigned thereto.

Related to the operation of the network, in certain case it may happen even with due care, messages sent to each other are revealed to unauthorised third parties during the use of the phone and the internet. In consideration of the above, the Customer acknowledges that there are risks associated with the use of the service for disposal, and the Customer has decided to use the service after having considered such risks. In this regard, the Bank shall not be held liable for information constituting bank secret being revealed to unauthorised third parties in the course of electronic communication for reasons beyond the Bank's control.

Budapest, 01.03.2021