SPECIAL CONDITIONS FOR ELECTRONIC BANKING PER WESTERN UNION DIGITAL BANKING APP

For ease of reading, these Special Conditions for electronic banking per Western Union Digital Banking App are not formulated in a gender-specific manner and apply equally to all genders.

For the purpose of these Special Conditions, the term "Account Documents" shall hereinafter mean all documents related to the onboarding process of the customer under the Western Union Digital Banking App, including but not limited to the Information Sheet provided by Western Union International Bank GmbH, General Terms and Conditions of Western Union International Bank GmbH, Special Conditions for debit card and virtual debit card, these Special Conditions, Special Conditions for SEPA instant payments and related price lists, as such may be applicable on a case by case basis, depending on the services to be performed by the Bank to the customer, together with any other ancillary documentation necessary for finalizing or implementation of the onboarding process under the Western Union Digital Banking App, as expressly and individually accepted by the customer and as amended from time to time.

1. General provisions

1.1. Usage of electronic banking per Western Union Digital Banking App (hereinafter referred to as „e-banking")

(1) These Special Conditions regulate the use of e-banking of Western Union International Bank GmbH acting through its Italian branch (hereinafter referred to as the "Bank") by the customer.

(2) The Western Union Digital Banking App (hereinafter referred to as the "App") is an app of the Bank that enables the customer, subject to compliance with the requirements agreed in these Special Conditions, to use a mobile terminal (e.g. smartphone) to make inquiries (e.g. account balance, turnover) and to issue orders (e.g. payment orders) as well as to make legally binding declarations of intent and other statements.

(3) e-banking is a form of internet banking as defined in the Annex to the Consumer Payment Account Services Ordinance (BGBl II No. 60/2018).

1.2. Condition for the use of the App

The possibility to use the App requires the existence of a business relationship between the Bank and the customer, and an agreement for e-banking between the customer and the Bank. The business relationship itself is governed by the Account Documents and the terms and conditions therein; in particular these special conditions govern the customer's use of e-banking via the App.

1.3. Registration in the App

Registration in the App is performed by following the steps provided by the App. One step in the registration process is the entry of the email address and Password that is (i) used by the customer to log into his/her wu.com profile or (ii) created by the customer when registering in the App. After setting-up the Username and Password, the customer has the option to activate biometrics or a Passcode.

1.4. Electronic signature in the App

To conclude the agreement with the Bank and use the App, the customer shall activate and use an advanced electronic signature or qualified electronic signature as set out in the Bank's Terms and Conditions on the use of the advanced electronic signature or qualified electronic signature.

1.5 Definitions

Password

The password is the secret word (combination of 8-16 characters with at least 1 uppercase, 1 lowercase and 1 number or special character) that is (i) used by the customer to log into his/her wu.com profile or (ii) specified by the customer when registering in the App. The password is a personal identification feature of the customer, which serves to identify the customer in e-banking if the e-mail address is also specified. The password can be changed by the customer in the App.

Passcode

The passcode is a six-digit number that can be created by the customer and used for log-in instead of the Password. Orders may be placed and legally binding declarations of intent or other statements may be made by entering the Passcode. For the purpose of control by the customer, details about the order to be authorized (e.g. IBAN of the recipient and the amount of the payment transaction) or about the legally binding declaration of intent or other declaration are displayed for this purpose.

Entering the Passcode is also required to access the App if strong customer authentication is required under the Austrian Payment Services Act 2018 or the Delegated Regulation (EU) 2018/389. The Passcode can be changed by the customer in the App.

Touch ID

Touch ID is a personal identification feature of the customer that enables identification in e-banking by means of a fingerprint and must be activated by the customer in the App. Touch ID is an alternative option to identifying the customer by e-mail address and Password. Orders may be placed and legally binding declarations of intent or other statements may be made by entering the Touch ID. For the purpose of control by the customer, details about the order to be authorized (e.g. IBAN of the recipient and the amount of the payment transaction) or about the legally binding declaration of intent or other declaration are displayed for this purpose. To use Touch ID, the customer must have a Touch ID-enabled mobile device (e.g. smartphone) and the customer must have Touch ID enabled.

Face ID

Face ID is a personal identification feature of the customer that enables identification in e-banking by means of facial recognition and must be enabled by the customer in the App. Face ID is an alternative option to identifying the customer by e-mail address and Password. Orders may be placed and legally binding declarations of intent or other statements may be made by entering the Face ID. For the purpose of control by the customer, details about the order to be authorized (e.g. IBAN of the recipient and the amount of the payment transaction) or about the legally binding declaration of intent or other declaration are displayed for this purpose. To use Face ID, the customer must have a Face ID-enabled mobile device (e.g. smartphone) and the customer must have Face ID enabled.

e-Postbox

The e-Postbox is the mailbox available for the customer to send notifications to the Bank in case of queries or if customer needs support and to receive notifications from the Bank.

Authentication code

The authentication code is a code that is generated during strong customer authentication as defined in the Austrian Payment Services Act and the Delegated Regulation (EU) 2018/389 and is dynamically linked to the step to be authorized (e.g., the order to be authorized or the customer's declaration of intent to be submitted). Each time the Passcode is entered, a unique authentication code is generated.

Strong Customer Authentication

Strong customer authentication is the strong customer authentication procedure regulated in the Austrian Payment Services Act 2018 and the Delegated Regulation (EU) 2018/389.

2. Access – Orders and declarations

(1) Access to e-banking is only granted to customers who have legitimized themselves by entering their e-mail address and Password or by Touch ID or Face ID or Passcode. The additional entry of the Passcode for access to the App is required if more than 30 days have elapsed since the last strong customer authentication or if the customer accesses his payment account for the first time.

(2) The placing of orders and the submission of legally binding declarations of intent or other declarations by the customer shall be effected by entering its Passcode, Touch ID or Face ID.

(3) Legally binding declarations of intent by the customer may also be made by the customer accepting an offer expressly made to him by the Bank in e-banking by declaring acceptance (e.g. by clicking on a box containing his declaration of consent) and subsequently confirming his acceptance (e.g. by pressing a button); the customer may also make other declarations in this way.

(4) The Bank is entitled, but not obliged, to execute transfers of the customer under the conditions of Articles 10 to 21 of the Delegated Regulation (EU) 2018/389 also without authorization by the Passcode, Touch ID or Face ID.

(5) Acceptance of orders by the Bank shall not be deemed to be a confirmation of execution.

3. Due Diligence and recommended security measures

3.1. Compliance obligation

Each customer is obliged to comply with the duties of care agreed upon in section 3.2. Customers who are entrepreneurs are additionally obliged to comply with the recommended security measures pursuant to Section 3.3. For customers who are consumers, the Bank recommends compliance with the recommended security measures, without consumers being obliged to comply. A breach of these obligations may, pursuant to Section 7 (in relation to consumers) or Section 8 (in relation to entrepreneurs), result in the customer's liability for damages or in the elimination or reduction of its claims for damages against the Bank.

3.2. Due Diligence obligations

3.2.1. Confidentiality and blocking obligation

(1) The customer shall keep its Password and Passcode secret; it may not disclose them to third parties or pass them on to third parties in any other way. However, disclosure to payment initiation service providers and account information service providers is permissible insofar as it is necessary for them to be able to provide their services to the customer.

(2) The customer is obliged to exercise the utmost care in the storage and use of his Password and the Passcode in order to avoid misuse. In particular, the customer shall ensure that its Password and the Passcode are not spied out during their use; the customer shall also not store them in his/her mobile device on which he/she has installed the App or note them electronically, for example in an app for notes, unless such storage or app is protected against access by third parties.

(3) In the event of loss of Password and/or Passcode, as well as if the customer has become aware of any misuse or other unauthorized use of e-banking, the customer shall immediately arrange for the blocking of access to its e-banking.

(4) In the event of loss or theft of the customer's mobile device on which the App is installed, the customer shall immediately arrange for the blocking of the customer's access to e-banking; this shall also apply if the customer has installed the App on several mobile devices and one of them is stolen or lost.

3.2.2. Due Diligence for locking the mobile device and during installation

(1) The customer is obliged to block access to the use of the mobile device on which the App is installed or access to data stored there for unauthorized persons if the customer does not use the device.

(2) The customer may install the App exclusively from the Apple App Store or the Google Play Store.

3.2.3. Due Diligence for orders and declarations

The data displayed in the App after entry by the customer must be checked for correctness by the customer before using the Passcode, Touch ID or Face ID. The Passcode, Touch ID or Face ID may only be used to place orders or make declarations if the data displayed in the App matches the desired order or the desired legally binding declaration of intent or other declaration.

3.3. Recommended security measures when using e-banking

(1) The customer is recommended to change the Password and the Passcode on his own on a regular basis, at least every two months.

(2) The customer is advised to immediately block access to e-banking if there is reason to fear that unauthorized third parties have gained knowledge of the Password and/or Passcode, or if there are other circumstances that could enable an unauthorized third party to misuse the Password and/or Passcode.

(3) The customer is recommended to secure his mobile device, on which the App is installed, against risks from the internet, in particular to keep it up-to-date, as well as to perform security updates of the operating system of the mobile device and to use an up-to-date virus protection.

4. Block

4.1. Automated block

(1) Access to e-banking is automatically temporarily blocked if the Password is entered incorrectly three times in a row during an access. After the first temporary block has been automatically lifted and if the Password is entered incorrectly twice in succession, a second temporary lockout will occur. After the second temporary lock is removed, each additional incorrect Password entry will result in a new temporary lock. The maximum total number of incorrect Password entries that will result in a temporary lockout is nine. After the tenth incorrect Password entry, access to e-banking will be automatically blocked permanently. The Bank will immediately notify the customer of the duration of the respective temporary block.

(2) Access to e-banking is automatically blocked permanently if the Passcode has been entered incorrectly five times in succession.

4.2. Block by the customer

The customer can block access to e-banking by entering the Passcode incorrectly five times in succession him-/herself or by telephone at any time at +390685960176.

4.3. Block by the Bank

(1) The Bank shall be entitled to block e-banking for a customer if objective reasons related to security justify this or if there is a suspicion of unauthorized or fraudulent use.

(2) The Bank shall inform the customer of any blocking of e-banking and the reasons therefor as far as possible before, but at the latest without undue delay after, the blocking, provided that the disclosure of the blocking or the reasons for the blocking would not violate a court order or an order of an administrative authority or be contrary to national or European law or objective security considerations.

4.4. Announcement and lifting of the block

(1) Before a block becomes permanent, the customer will receive a warning.

(2) The Bank shall lift a block pursuant to section 4.3. as soon as the reasons for the block no longer exist. The Bank shall inform the customer of the lifting of the block without undue delay.

(3) The customer may request the lifting of a block at any time by telephone at +390685960176.

5. Legally binding orders and declarations of the customer

(1) Orders and legally binding declarations of intent as well as other declarations made by the customer in e-banking shall be deemed to have been issued or made by the customer if the customer has released them by means of the Passcode, Touch ID or Face ID. The Customer may also make declarations of intent in the manner set forth in Section 2 (3).

(2) The Bank shall not be obliged to obtain a confirmation of the order or the legally binding declaration of intent or any other declaration. The right of the Bank to obtain an order confirmation as agreed in Section 4 of the "General Terms and Conditions of Western Union International Bank GmbH" (hereinafter referred to as "GTC") shall remain unaffected thereby.

(3) Orders and legally binding declarations of intent as well as other declarations by the customer may only be issued or made using the App to the extent that they are covered by an authorization of disposal pursuant to Section 32 GTC.

6. Time of receipt/ Execution of payment orders

(1) Time of receipt of payment orders: The time at which a payment order is received by the Bank via e-banking shall be deemed the time of receipt. If the payment order is received on a business day after the cut-off time or not on a business day of the Bank, the order shall be treated as if it had been received by the Bank on the next business day.

(2) The cut-off time for payment orders on a business day is specified in section 3.2 of the "WUIB Information Sheet".

(3) Payment orders: If the customer does not provide a future execution date, the payment order shall be executed on the same day if the payment transaction data is available for processing by the Bank's acceptance deadline at the latest. Otherwise, the execution shall take place no later than on the business day following the day of data transmission by the ordering party. The prerequisite for execution is sufficient account coverage (credit balance or overdraft facility).

(4) Additionally, Sections 36 and 36a GTC shall apply where transfer orders are regulated.

7. Liability of the customer as a consumer

(1) The customer who is a consumer shall be liable for the entire loss of an unauthorized payment transaction caused to the Bank (i) by the customer's intentional or grossly negligent breach of the duties of care pursuant to Section 3.2 or (ii) with the intent to defraud.

(2) If the breach of the due diligence obligations pursuant to Section 3.2. is due to slight negligence on the part of the customer, the customer's liability shall be limited to a maximum of EUR 50. If the customer has breached the duties of care pursuant to Section 3.2 neither fraudulently nor intentionally, the type of personalized security features and the particular circumstances under which the misuse of e-banking took place shall be taken into account in any division of damages between the customer and the Bank.

(3) If the loss or theft of the mobile terminal on which the App is installed or the misuse of e-banking was not noticeable to the customer prior to the payment, the customer shall not be liable in the event of a slightly negligent breach of the duties of care pursuant to Section 3.2. The customer shall also not be liable in the event of a slightly negligent breach of the due diligence obligations pursuant to Section 3.2 if the loss of the personal identification features was caused by acts or omissions of the Bank (including its employees and agents and other entities to which such services have been outsourced).

(4) Notwithstanding Section 7 (2), the customer shall not be liable if the Bank did not require strong customer authentication in case of misuse of e-banking or in case of an unauthorized payment via e-banking. If an unauthorized payment transaction was fraudulently facilitated by the customer, the customer shall be liable irrespective of whether the Bank required strong customer authentication or not.

(5) The customer shall not be liable if the damages resulted from a non-authorized use of e-banking after the customer has informed the Bank of a loss, theft or misuse in accordance with section 3.2.1(3) or section 4, unless the customer acted with fraudulent intent.

8. Liability towards entrepreneurs/Liability of the customer as an entrepreneur

In relation to entrepreneurs, section 68 of the Austrian Payment Services Act 2018 shall be waived in its entirety; the Bank's liability for damage caused by slight negligence shall be excluded. The Bank shall not be liable, irrespective of the degree of fault, for any damage caused in connection with the customer's hardware or software or caused by the failure to establish a connection with the Bank's data processing center or caused by a temporary failure of the Bank's facilities for processing e-banking, or if the entrepreneur has breached the duties of care set forth in Section 3 or if the entrepreneur has failed to comply with the recommended security measures set forth in Section 3. If the entrepreneur has breached the duties of care set forth in Section 3 or has failed to comply with the recommended security measures contained in Section 3, the entrepreneur shall be liable to the Bank for the resulting damage.

9. Declarations and communication

(1) The customer shall receive legal declarations, notices and information from the Bank (hereinafter jointly referred to as "Declarations") in a form of communication agreed with the customer. The forms of communication agreed upon are e-mail, SMS, push notifications and transmission to the customer's e-Postbox with notification of the customer. If the customer and the Bank conclude agreements on other forms of communication, their effectiveness shall remain unaffected by this provision; this shall also apply to communication per App. The effectiveness of written declarations (including those sent by mail) shall also remain unaffected.

(2) The Bank may transmit declarations to the customer to the e-mail address provided by the customer to the Bank. Declarations made by the Bank to the customer by e-mail to this e-mail address shall therefore be effective. The customer may also communicate with the Bank by e-mail and make effective declarations by e-mail and via the e-Postbox in the App.

The customer cannot communicate with the Bank and make effective declarations if the customer is informed in an e-mail that it is not possible to reply to this e-mail address ("no-reply addresses").

(3) In the event of a change of its e-mail address, the customer shall notify the Bank of its new e-mail address without undue delay; this shall be possible by telephone at +390685960176 or in the App. If the customer has not notified the Bank of his/her changed e-mail address and if the Bank receives information that the e-mail address is no longer current, declarations by the Bank shall be deemed to have been received by the customer if the Bank has both sent them to the last e-mail address notified by the customer and has transmitted them to the customer's e-Postbox with notification of the customer; if the Bank has not received such information, declarations by the Bank shall be deemed to have been received by the customer if the Bank has sent them to the last e-mail address notified by the customer.

10. Change of the Special Conditions for ebanking per Western Union Digital Banking App

(1) Amendments to these Special Conditions shall be offered to the customer by the Bank provided that there is an objectively justified reason, not later than two months before their proposed date of entry into force; the provisions affected by the amendment offer and the proposed amendments to these Special Conditions shall be presented in a comparison (hereinafter "Comparison") attached to the amendment offer. The amendment offer shall be communicated to the customer by sending a notice, headed *"Proposal for unilateral amendment of the contract" ("Proposta di modifica unilaterale)"*, describing the content of the proposed change(s) via email or other durable means previously agreed by the customer pursuant to Section 27 of the GTC. The customer shall be deemed to have consented to the amendments if the Bank does not receive an objection from the customer before the proposed date of entry into force via email, mail or other durable medium agreed by the customer pursuant to Section 27 of the GTC. The Bank shall draw the customer's attention in the amendment offer to the fact that the customer's silence by failing to object in writing or electronically [e.g. via e-mail or the App], as the case may be, shall be deemed consent to the amendments and that the customer, who is a consumer, shall have the right to terminate the agreement on e-banking per Western Union Digital Banking App and the Account Documents for which e-banking per Western Union Digital Banking App is agreed, without notice and free of charge before the amendments enter into force. In addition, the Bank shall publish the Comparison as well as the complete version of the new special conditions for e-banking per Western Union Digital Banking App on its website and shall send the customer via e-mail the complete version of the new special conditions; the Bank shall also refer to this in the amendment offer.

(2) The notification and amendment offer in accordance with paragraph (1) of Section 11 shall be provided to the customer via transmission of the amendment offer together with the Comparison via e-mail or other durable means previously agreed by the customer pursuant to Section 27 of the GTC. The notification shall be made in such a way that the Bank can no longer alter the amendment offer unilaterally and the customer has the opportunity to additionally store and print out the notification for him-/herself. The amendment offer shall be deemed to have been received by the customer at the time when the customer receives the notification and is able to retrieve such information under ordinary circumstances.

(3) The modification of the Bank's services by means of an amendment to these Special Conditions pursuant to paragraph (1) of Section 11 shall be limited to objectively justified cases; an objective justification shall be deemed to exist,

(i) if the amendment is required by a change in the statutory provisions governing payment services and their settlement or by requirements of the Financial Market Authority, the European Banking Authority, the European Central Bank, the Austrian National Bank or any other competent authority,

(ii) if the change is necessitated by the development of case law relevant to payment services and their settlement,

(iii) if the amendment promotes the security of banking operations or the processing of the business relationship with the customer for e-banking,
(iv) if the amendment is necessary to implement technical developments or to adapt to new programs for the use of mobile devices or the App,
(v) if the change is necessitated by a change in the legal requirements for placing orders and making declarations in the App,
(vi) if the change is necessitated by a change in the legal provisions for those banking transactions that the customer can conduct in the App.

The introduction of fees and the change of agreed fees by an amendment of these Special Conditions are excluded.