This English translation is provided for your convenience only. In the event of discrepancies the German original text shall prevail over the English translation.

A GENERAL PROVISIONS

1 GENERAL INFORMATION

1.1 Online banking (OnlineBanking or 24You) is a special service product from UniCredit Bank Austria AG (hereinafter "the Bank" in short). It enables a customer (as holder of a current account or a securities account or authorised signatory on such an account) to communicate with the Bank's data processing centre by means of data transmission via the Internet and, after electronic authorisation, to access information, instruct the Bank to execute orders relating to current accounts and securities accounts, and, in particular, to make declarations of intent to the Bank via mailbox of the online banking system; the customer can also request information about current accounts and securities accounts to be transmitted to him/her by push message in online banking apps issued by the Bank, e.g. MobileBanking app, or e-mail, and s/he can obtain information by telephone. A version of online banking (e.g. "MobileBanking") optimised for mobile devices (e.g. smartphones and tablets) may also be used as part of online banking. The customer himself/herself can select specific settings in the "Security" section of "Administration" in the online banking system, e.g. register his/her mobile device.

1.2 The "Agreement on Participation in Bank Austria online banking" (hereinafter "the Agreement" in short) is concluded between the Bank and the customer for an indefinite period. The Agreement entitles the customer to use the online banking service. The customer will then be permitted to access all current accounts and securities accounts held by him/her via the online banking service. If the current/securities account holder wishes to allow an authorised signatory to access the account by means of online banking, s/he must issue such authorisation in writing. For joint current/securities accounts, all current or securities account holders must issue their authorisation before an authorised signatory is permitted to access the account via the online banking service. No online banking transactions may be conducted via current/securities accounts for which joint signing authority was agreed, the online banking authorisation for these accounts is limited to calling up account information.

2 DEFINITIONS

2.1 User Code (user identification/UI):
Every customer receives a unique user code comprising several digits, which enables the Bank to assign a customer to the current/securities accounts which s/he is authorised to access via online banking. The Bank will inform the customer of the user code when s/he signs the Agreement. The user code may not be changed by the customer.

2.2 Personal Identification Number (PIN):
The PIN must be used when logging into online banking. Every time the customer logs into online banking, the customer must verify his/her identity by providing the user code, the PIN and (if requested by the bank) a TAN generated for the specific individual case at the same time.
The PIN is either handed to the customer personally in a sealed envelope after s/he has signed the Agreement, or is mailed to him/her upon his/her express request.
The customer may change his/her PIN code for online banking whenever s/he wishes by using a TAN or the ATC.
The customer will have to enter the changed PIN code whenever s/he logs into the online banking system.
For security reasons, the Bank may ask the customer to change to a longer or safer PIN when logging into online banking. Depending on the content of the request, the customer is obliged to comply with such a request after a certain maximum number of logins (at least three) or on the first login after a specific period of at least 8 weeks in order to log into online banking. The number of logins and/or the deadline after which the change of PIN is mandatory will be notified to the customer upon the first request to change the PIN. The Bank will remind the customer of the need to change the PIN on each subsequent login to online banking. Alternatively, the customer may request a new PIN code at any of the Bank's branches during business hours. The new PIN code will be given to the customer personally at a Bank branch of his/her choice, or mailed to him/her upon his/her express request.

2.3 Transaction Number (TAN):
TAN is an authentication code generated in a specific individual case, which must be used when logging into online banking (in addition to the user code and PIN) and for issuing orders and other legally binding declarations of intent towards the Bank within the framework of online banking. An instruction is considered to have been issued and a declaration of intent is deemed to have been made as soon as the TAN is used in the designated field and the button intended for the purpose is pressed.

The Bank may refrain from requesting the use of a TAN when logging into online banking unless the customer logs onto online banking with a new device or browser for the first time or the last login using a TAN was over 90 days ago. If the customer logs into online banking without using a TAN and there are no additional security features such as the binding on a specific mobile device, he/she may only access information on account balance as well as the payment transactions of the last 90 days in online banking.

The Bank provides the customer with different TAN systems for the use of online banking. If the Bank can no longer provide a TAN system used by the customer because

- in connection with the security of the relevant TAN system, or of the systems for which it is used, there are objective grounds for such discontinuation or
- due to legal or regulatory provisions, the Bank may no longer provide a TAN system that is used by the customer,

the Bank will inform the customer of the reasons for such discontinuation and offer the customer to switch to another TAN system with a higher security standard free of charge, unless the customer already uses a TAN system with a higher security standard which has been activated for him/her. The Bank will inform the customer of such offer in a timely manner using the channel agreed in the context of the business relationship promptly enough so that it is sent to him/her no later than two months prior to the proposed time to switch to another TAN system. This offer is deemed to be accepted by the customer if no objection from the customer is received by the Bank prior to the proposed time of the switch; the Bank will refer in its notification to the consequences of his/her silence as well as the customer's right to free termination in accordance with Section 12.3.
If the customer does not accept the Bank's offer by raising an objection and does not use his/her right to terminate the Agreement, effective starting from the time the TAN system used by the customer is not provided anymore, s/he will only be able to continue using those online banking functions for which no TAN is required. This is the case for access to information on the account balance of his/her accounts authorised for online banking and on the payment procedure of the last 90 days, provided that since the last login without a TAN entry no more than 90 days have elapsed and the bank waives the requirement to use a TAN on each login to online banking.
If the customer refuses the offered switch to a different TAN system with a higher security standard, the providing of the TAN system used by the customer will be stopped at the earliest four months after notification of the offer to switch.
Despite an objection, the customer may switch to the TAN system with a higher security standard offered at any time until the TAN system he/she uses is finally stopped. The customer may inform the Bank of his/her request to switch to the TAN system offered either personally at a branch or in writing by post.
The customer can decide whether s/he wishes to use a mobileTAN or a CardTAN in online banking. Within the various TAN systems activated for the customer, s/he can decide to make alternate use of these different TANs.

a) mobileTAN:
If the customer wants to use the mobileTAN system, s/he can inform the Bank either personally at any of the Bank's branches or by writing a letter. If the customer uses the mobileTAN system, s/he receives the mobileTAN required for logging in to-online banking, signing an online banking transaction or submitting a declaration of intent by means of SMS (Short Message Service) or push message (message to the online banking app used by the customer, e.g. MobileBanking app) on a mobile device (such as mobile phone or tablet). If the mobileTAN is to be sent via SMS, the customer must inform the Bank – personally at a branch and in time before the first use of the mobileTAN system – of the telephone number of the mobile phone used for this purpose.

The customer can change the number to which the mobileTANs are sent via SMS personally at a branch of the Bank or, if an SMS can be sent to the customer to the previously used mobile phone number known to the Bank, using a mobileTAN via online banking. The customer can use a valid mobileTAN in online banking to switch between delivery of mobileTANs by SMS or by push message. For security reasons, the Bank may suspend the possibility of changing the mobile phone number and changing the method of delivery via online banking if this is justified on objective grounds in connection with the safety of personal identification details or the systems for which they can be used.
The message with the mobileTAN sent to the customer also includes information on the transaction to be completed (especially in the case of payment orders: International Bank Account Number/IBAN or account number of payee, Bank Identifier Code/BIC or routing code of payee bank, and transfer amount) that is to be verified by the customer.

A mobileTAN can only be used to sign the transaction for which it was requested. If an order is changed after a mobileTAN has been requested for it, the mobileTAN sent before the change is no longer valid. A new mobileTAN must be requested. A mobileTAN is rendered invalid once it is used.
When using the mobileTAN procedure, the customer is required to check the data relating to the order (e.g. IBAN of the payee's account, transfer amount), which are sent by the message together with the mobileTAN, to ascertain that they correspond with his/her order. The customer may only use the mobileTAN if such data correspond with the order.

Delivery of the mobileTAN via SMS:
The customer can receive an SMS with a mobileTAN on his/her mobile telephone only when the basic requirements for the receipt of SMS messages are met, for example,

- the telephone must be capable of receiving SMS messages,

- the service contract with the mobile communications provider must include the receipt of SMS messages, and
- the customer must be in an area in which his/her mobile communications provider delivers SMS messages.

Delivery of the mobileTAN via push message: The customer can receive a push message with a mobileTAN on a mobile device such as a smartphone or a tablet only when the basic requirements for the receipt of push messages are met, for example:

- a current version of the online banking app of Bank Austria used by the customer is installed,
- the device has been activated in the device management function of the Bank's online banking app used by the customer and is capable of receiving the mobileTAN push,
- the customer is in an area where there is an Internet data connection via the customer's mobile phone provider or through WLAN via a network operator.

b) CardTAN:
If the customer wants to use the CardTAN system, s/he has to inform the Bank of his/her intention either personally at any of the Bank's branches or by writing a letter or – if s/he has already made an agreement with the Bank on use of the mobileTAN system – electronically via online banking by using a mobileTAN. To use the CardTAN system, the customer needs an active (i.e. neither blocked nor expired) CardTAN-enabled debit card issued by the Bank (e.g. a Maestro card issued by the Bank) and a special card reader (CardTAN generator). A CardTAN generator can be requested by the customer directly from the Bank.

When the debit card is inserted in the CardTAN generator, specific data of the login or transaction to be executed via online banking are recorded and processed in the CardTAN generator via an optical interface (see "Flicker" mode) or through manual input. A programme stored on the chip of the debit card will then generate a CardTAN. The customer must enter the CardTAN in the online banking system and the Bank will verify it. The CardTAN generator can be used in the "Flicker" mode or in the "manual input" mode. "Flicker" mode is the simpler mode. If the customer encounters problems with the use of the Flicker code, s/he can switch to "manual input on the CardTAN generator" by using an option available in the online banking system.

"Flicker" mode: The Bank server transmits the required data, in particular the transaction details, needed for calculating the CardTAN from the screen of the customer's input device (e.g. computer, tablet, etc.) to the CardTAN generator via optical interfaces by means of a flashing black-and-white graphics. The transaction details representing the transaction to be authorised by the customer will be displayed on the CardTAN generator for verification by the user. When using the CardTAN system in the "Flicker" mode, the customer is required to check the transmitted transaction details (e.g. in the case of payment orders: IBAN of the payee's account, transfer amount) to ascertain that they correspond with his/her order. The customer may only use the CardTAN if the transaction details correspond with his/her order.

"Manual input" mode: The customer is required to use the CardTAN generator to enter specific transaction details, in particular the transaction data, requested on the online banking input template. A description of the steps required for manual input is available in a help menu directly in the online banking system or in the operating instructions of the CardTAN generator. When using the "manual input" mode, the customer is required to check the input details to ascertain that they correspond with his/her order. The customer may only use the CardTAN generated for this transaction if the transaction details correspond with his/her order. A CardTAN can only be used for executing the transaction for which it was generated. If a transfer order is changed after the CardTAN was generated, this CardTAN can no longer be used. In this case a new CardTAN must be generated with the CardTAN generator. A CardTAN is rendered invalid once it is used.

2.4 Authorisation code (= ATC):
An ATC is an authorisation code that the customer needs to set up in the Mobile Banking App from Version 7 onward, which can then be used for issuing orders and other legally binding declarations of intent towards the Bank within the framework of online banking. An instruction is considered to have been issued and a declaration of intent is deemed to have been made as soon as the ATC has been entered in the designated field and the relevant button has been confirmed. As part of the authorisation, a specific protected key (hash value/code) is generated in the app based on the respective order data and confirmed by the customer with ATC. The customer's order is only processed further by the bank if the order data based on the key match the order data on the bank server. If a saved order has been changed, a new order-specific key must be generated before signature, and confirmed again with ATC and the order data must be newly compared.
Before entering the ATC, the customer is obliged to check that the order data displayed in the app for control purposes (e.g. IBAN of the payee's account and transfer amount) match his/her order and may enter the ATC to sign the order only in the event that the order data match.

2.5 Mobile Token:
A Mobile Token is a one-time code that can be used to register a new mobile device for use of the

MobileBanking app (from version 7 onward). A Mobile Token is requested by using the ATC.

2.6 Biometric data:
When using the Bank's online banking apps on mobile devices (smartphone or tablet) – depending on the technical capacity of the mobile device– the customer can choose to use biometric data (such as fingerprints or FaceID) instead of the PIN and/or ATC. In this case, the customer's verification by means of his biometric data replaces entry of the PIN and the ATC.

2.7 Personal Identification Details:
The user code (UI), Personal Identification Number (PIN), Transaction Numbers (TAN), ATC, mobile Token as well as biometric data form the personal identification characteristics of a customer for online banking.

2.8 Single Password System:
The Bank uses the single password system for its online banking services, and for some other service products which require the use of a user code. This means that a customer only receives one user code (see Section 2.1) and one PIN (see Section 2.2), which are to be used for all current/securities accounts which the customer is authorised to use for online banking transactions (and for other service products for which a user code is required). If the user code is blocked, the customer is unable to conduct any transactions for which the user code is normally required.

3 AUTHENTICATION
The Bank verifies the customer's authorisation to use online banking on the basis of the personal identification details.

4 TRANSACTIONS VIA ONLINE BANKING
4.1 Transactions can generally be completed and declarations of intent submitted to the Bank through the online banking system 24 hours a day, 7 days a week. As maintenance work occasionally has to be carried out at the Bank's data processing centres, a service window is provided from 7:00 p.m. to 6:00 a.m. Online banking services may not always be available during this time if maintenance work is in progress. The Bank will inform customers in a timely manner of any maintenance work to be carried out through appropriate notification in online banking and on the Bank's website.

4.2 The customer establishes a link with the Bank's data processing centre by logging into the online banking system via the Bank's website by entering his/her user code, PIN and the TAN generated for the individual case. The customer will then be presented with the available transactions in the online banking system, and selects the desired transactions. The customer must then enter the information requested by the system into the screen for submission over the Internet. When issuing a transfer order, the customer must in each case state the payee's customer identifier. Any additional information provided by the customer on the payee, such as the payee's name or the reason for payment, is not part of the customer identifier and therefore merely serves as documentation and is not considered by the Bank when it carries out the transaction. The customer is then required to complete the transaction by entering the valid TAN generated for the respective transaction or by entering the ATC and clicking on the designated button for confirmation.

4.3 The time of receipt is the time at which a transaction order is received by the Bank via online banking. If a transaction is received via online banking on a day other than a bank business day or after a time close to the end of a bank business day, the transaction will be treated as if it had been submitted on the next bank business day. The Bank publishes these times in the "Information provided by UniCredit Bank Austria AG on Payment Services for Consumers", which can be viewed on the Bank's website or, upon a customer's request, are available in printed form at any Bank branch or can be sent to him/her by regular mail.
A customer can also arrange for an order to be executed on a specified future date (forward order). If this forward date is not a bank business day, the order will be treated as if it had been received on the following bank business day.

4.4 A customer may submit as many transfer orders as s/he wishes for an account via online banking. The Bank is only obliged to carry out a transfer order if complete coverage is available on the customer's respective account. This means that for a payment account with basic features (basic account), customers may submit transfer orders via online banking only within the limit of a credit balance available in the account. The customer can also combine multiple transfer orders and approve them with a single TAN or with a single entry of the ATC.

4.5 General information on limits:
4.5.1 In the online banking system it is possible to set daily limits or transaction limits. A daily limit is the total amount up to which transfer orders may be given on any single calendar day. The daily limit applies to all transfer orders (except transfers between the customer's own accounts and orders relating to securities) given by the customer on any single calendar day, irrespective of the execution/accounting date. A transaction limit is the amount up to which a transfer order may be given alone or together with other transfer orders (except transfers between the customer's own accounts and orders relating to securities) using a single TAN or a single entry of the ATC.

4.5.2 A limit may be set by the Bank unilaterally (see Section 4.5.3) or it may be agreed between the Bank and the customer. In both cases the limit is referred to as a "bank-side limit".

4.5.3 The Bank may introduce or lower a bank-side limit without participation of the customer if

- this is justified on objective grounds in connection with the safety of personal identification details or the systems for which they can be used;
- it is suspected that unauthorised orders have been issued, or that personal identification details are being fraudulently used.

The Bank will inform the customer of the introduction or lowering of a bank-side limit and also the reasons for such introduction or lowering, in the form agreed with the customer, before the bank-side limit is introduced or lowered if possible, or immediately afterwards.

4.5.4 Within any bank-side limit (see Section 4.5.2) the customer may set a personal transaction limit directly in the online banking system at any time by using a valid TAN or the ATC.

4.6 An authorised transfer order cannot be cancelled once it has been received by the Bank via the online banking system. A forward order that has been received by the Bank can be cancelled by midnight of the business day before the agreed execution date directly in the online banking system using a valid TAN or the ATC.

4.7 eps online transfer:
Customers using the online banking system may also submit eps online transfer orders. An eps online transfer order is a standardised payment procedure for purchases on the Internet and for the use of E-Government services. In this context the customer can use his/her user code and PIN and a TAN to directly log into online banking on the Internet shop website or on the E-Government website, which are in each case marked with a logo for eps ("e-payment standard") and online transfer, and then make the payment by submitting a transfer order. An eps online transfer order is confirmed like any other transfer order via online banking by using a TAN or the ATC.

The processing of eps online transfers does not involve any third-party request for entering bank-specific data of the customer, or any temporary storage of such data, because the customer logs into online banking directly on the Bank's website or in Bank Austria's MobileBanking app and confirms the transfer order there. When processing an eps online transfer, the Bank will not transmit to the merchant any bank-specific data of the purchaser.

When the customer confirms an eps online transfer order, the Bank will guarantee execution of the transfer vis-à-vis the Internet merchant or the E-Government authority, which means that the customer cannot cancel such an eps online transfer order.
The eps online transfer is just an instrument which a customer may use to make a payment via the Internet through an online banking transfer order. Use of the eps online transfer service will not affect the contractual relationship between the customer and the merchant. For this reason, no objection may be raised against the Bank under the underlying transaction.

5 OBTAINING INFORMATION BY TELEPHONE
5.1 Telephone enquiries must be sent to the contact details specified in the online banking. For telephone enquiries by means of video call, the function provided for this in online banking must be used. After establishing the telephone connection with the Bank, the customer enters the user code and the two digits of the first five digits of the PIN which the Bank's employee requests.

5.2 The personal identification details provided by the customer will be checked. If they are correct, the requested information on the customer's own transactions, or on transactions for which the customer is authorised to use online banking, will be provided by telephone. Giving orders by telephone is not possible.

6 ACCOUNT INFORMATION SERVICE PROVIDERS AND PAYMENT INITIATION SERVICE PROVIDERS
6.1 The customer may grant specific account information service providers and payment initiation service providers access to one or more of his/her payment accounts authorised for online banking when the customer uses the services of these service providers.

6.2 Account information service providers offer consolidated information on one or more payment accounts of an account holder that can also be managed at different banks. Payment initiation service providers initiate a payment order at the request of an account holder with respect to a different payment account, which can also be managed by another credit institute.

6.3 If the customer uses the services of account information service providers or payment initiation service providers by allowing these service providers access to his/her payment account(s), under the terms of the Delegated Regulation (EU) 2018/389 on technical regulation standards for strong customer authentication and common and secure open standards for communication, the Bank is obliged to communicate with these service providers in a secure way and to allow them to rely on the authentication procedures for verification of the customer's identity.

7 DUE CARE

7.1 The customer is obliged, also in his/her own interest, to keep his/her PIN, TAN, ATC and mobile Token secret and not to disclose this information to any other persons (including the Bank's employees), except for the digits of the PIN requested for the purpose of authentication pursuant to Section 5.1. The use of biometric data (see Section 2.6) does not discharge the obligation to keep PIN, TAN, ATC or mobile Token secret. The ban on disclosure of PIN, TAN or ATC does not exist vis-à-vis account information service providers and payment initiation service providers whose services the customer uses. As soon as the customer suspects that another person has knowledge of his/her PIN or ATC or has made an unauthorised use of online banking, s/he must change the PIN or ATC immediately. For security reasons, the customer is recommended to change his/her PIN and ATC regularly (e.g. every two months) without being prompted to do so.
The customer must report the unauthorised use of online banking to the online banking hotline immediately (see Section 9.1). In the event of theft or loss of the mobile phone used to receive mobileTAN, the customer is recommended to block his/her mobile phone immediately. In the event of theft or loss of the mobile device phone, on which an online banking app is installed or is used to receive mobileTAN, the customer is recommended to block his/her mobile phone device and/or SIM card immediately.

7.2 If the URL of the login page in the browser address bar does not begin with https://online.bankaustria.at/ or https://banking.bankaustria.at/ or for browser-based mobile online banking does not begin with https://mobile.bankaustria.at/ , or if the padlock icon that indicates an encrypted connection is not shown in the browser window, this indicates that the customer is not on the Bank's website. In this case there is a risk that the website was created by unknown persons for the purpose of coaxing personal identification details out of the customer (phishing). In such a case the Bank recommends aborting the login and contacting the online banking hotline as quickly as possible (see Section 9.1) if one or several identification details were already entered on that website.

7.3 When using the mobileTAN system, the customer must check the order information (e.g. in the case of payment orders: IBAN of the payee account, the transfer amount) included in the message containing the mobileTAN to ensure that it matches the order that s/he wishes to submit and must only use the mobileTAN when the order information matches.
When using the CardTAN system in the "Flicker" mode, the customer is required to check the transmitted transaction details (e.g. in the case of payment orders: IBAN of the payee account, transfer amount) to ascertain that they correspond with his/her order. The customer may only use the CardTAN if the transaction details correspond with his/her order.
When using the CardTAN system in the "manual input" mode, the customer is required to check the transaction details entered by him/her at the CardTAN generator to ascertain that they correspond with his/her order created in the online banking system. The customer may only use the CardTAN generated for this transaction if the transaction details correspond with his/her order.
When using the ATC process, the customer is obliged to check before entering the ATC that the order data displayed in the app for control purposes (e.g. in case of payment orders: the IBAN of the payee's account and the transfer amount) match his/her order and may only enter the ATC to sign the order if the order data match.

7.4 When using the system, the customer is obliged to comply with the terms of use for online banking contained in these Terms and Conditions, and especially to correctly enter the customer identifier (see Section 4.2) when submitting orders and to only submit orders if the amount of the order is within the drawing limit of the respective account.

8 CORRECTION OF UNAUTHORISED PAYMENT TRANSACTIONS

In the event that an unauthorised or incorrectly executed payment is debited from the customer's account, proceedings to have the payment corrected by the Bank can only be initiated when the Bank is informed of the unauthorised or incorrectly executed payment immediately as soon as the customer gains knowledge of the fact, in any case not later than 13 months after the date of the payment, unless the Bank did not provide the customer with information, or access to information, on the respective transfer order or payment against his/her account (reference number, amount, currency, fees, interest, exchange rate, value date) in the form agreed with the customer. This does not preclude any other claims of the customer for correction.
In the case of an unauthorised payment transaction, the bank will refund the customer the amount of the unauthorised payment immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction. The refund is made by restoring the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. The amount on the payer's payment account will be valued no later than the date the amount had been debited. If the bank has informed the Financial Market Authority of justified reasons for there being the suspicion of the customer acting fraudulently, in writing, then the bank will immediately review and meet its refund obligation if the suspicion of fraud cannot be confirmed. Where the unauthorised payment transaction was initiated through a payment initiation

service provider, then the bank is obliged to make the refund.

9 BLOCKING

9.1 Every current/securities account holder and authorised signatory can have his/her user code blocked as follows:

- by telephone at any time by contacting the Bank's online banking hotline, the number of which can be viewed by the account holder on the website www.bankaustria.at, or
- personally or in writing at any Bank branch during the branch's opening hours.

A request to block a user code that is submitted at a branch during its business hours or at any time via the online banking hotline becomes effective immediately. Written blocking requests received by the Bank outside its business hours will take effect immediately after it next opens for business.

9.2 The Bank is authorised to block a user code independently of the customer if

- there are objective grounds to do so with regard to the security of the personal identification details or the systems for which they can be used;
- there is reason to believe that unauthorised orders have been submitted, or that the personal identification details have been used for fraudulent purposes.

The Bank will inform the customer of the blocking of the user code and also the reasons for such blocking (if this is not in violation of Austrian or Community law, a court order or an order issued by an administrative authority, or runs counter to objective security considerations) in the form agreed with the customer before the user code is blocked if possible, or immediately after such blocking.

9.3 If an incorrect PIN, TAN or ATC is entered four times in succession, the user code will be blocked immediately after the fourth incorrect entry.

9.4 The customer may request the unblocking personally. The unblocking may be requested in every communication way agreed with the bank (especially via the online banking hotline or in a Bank branch).

9.5 The bank is entitled to deny a payment initiation service provider or an account information service provider access to the customer's payment account if this is justified by objective and duly evidenced reasons associated with unauthorized or fraudulent access to the payment account by that payment initiation service provider or that account information service provider, including the unauthorized or fraudulent initiation of a payment transaction. The bank will immediately inform the customer – to the extent that notification of such blocking or of the reasons for such blocking would not infringe a court order or an order issued by an administrative authority, or contravene Austrian or Community law or objective security considerations – that the access to the customer's payment account by that payment initiation service provider or that account information service provider is denied and the reasons therefor by using one of the methods of communication agreed with the customer, before access is denied and at the latest immediately thereafter.

10 EXPIRY AND CANCELLATION OF THE AUTHORISATION

10.1 When an account is terminated, all online banking authorisations for the account expire automatically. When a holder of a current account or a securities account or an authorised signatory is no longer authorised to sign singly on a current account or a securities account, the online banking authorisation in respect of such account or securities account will also expire.

10.2 Every customer may terminate the Agreement in writing subject to one month's notice. Every current/securities account holder may revoke the online banking authorisation of an authorised signatory in writing or personally at any of the Bank's branches.

10.3 The Bank may terminate the Agreement at any time, without stating any reasons, subject to two months' notice; such termination must be communicated to the current/securities account holder on paper or on another durable medium as agreed.

By way of derogation from the above, if the customer maintains a "payment account with basic features" ("basic account") at the Bank, the Bank may terminate the Agreement subject to two months' notice only if

- the basic account has not been used for any payment transactions in more than 24 consecutive months; or
- the customer no longer has lawful residence in the European Union; or
- the customer has opened a second payment account at a bank domiciled in Austria which enables him/her to use the services specified in Section 25 (1) of the Austrian Consumer Payment Accounts Act (Verbraucherzahlungskontogesetz – VZKG); or
- the customer has been charged, pursuant to Section 210 (1) of the Austrian Code of Criminal Procedure (Strafprozessordnung – StPO), with a punishable offence committed to the detriment of the Bank or any of its employees; or
- the customer has repeatedly used the basic account for business activities within the meaning of Section 1 (1) 1 and (2) of the Austrian Consumer Protection Act (Konsumentenschutzgesetz – KSchG), Federal Law Gazette No. 140/1979; or

- the customer has refused a change to these Terms and Conditions which the Bank has offered to all holders of payment accounts with basic features (basic account).

10.4 The Agreement may be terminated immediately without notice by the customer or the Bank for important reasons. This shall especially be the case when the customer has made his/her personal identification details available to another person.
By way of derogation from the above, if the customer holds a basic account at the Bank, the Bank may only terminate the Agreement without giving notice, and with immediate effect, if

- the customer has intentionally used the basic account for unlawful purposes; or
- the customer has provided false information in order to be able to open the basic account; if s/he had provided correct information, s/he would have been refused the right to open a basic account.

10a PERSONAL FINANCE MANAGER

10a.1 The Bank shall provide the Customer with a personal financial manager (PFM) free of charge as part of their online banking. The PFM is automatically activated in online banking.

10a.2 The PFM classifies all payment transactions (current accounts and credit cards) over the last 24 calendar months into various expenditure categories for housing, food, transport, etc. After logging into online banking, the customer is shown a breakdown by category, based on the value of payment transactions, budgeting and, if relevant, the customer's savings targets. The classification is applied automatically and is merely a suggestion that the customer can adapt how he/she wishes and use for his/her own purposes (e.g. setting and checking a budget).

10a.3 The automated classification carried out by the PFM is used solely to support the customer's personal financial planning in online banking. The PFM data is not used for any other purposes, and is visible only to the customer. If a customer would like specific customer advice or individual product offers based on the PFM data, he/she would need to explicitly grant the bank his/her consent (which can be revoked at any time) to process the PFM data for the purposes of providing individual customer advice or creating and sending personalised product offers.

10a.4 No personal data from the PFM will be forwarded to third parties.

10a.5 Changes and extensions to the PFM's functionality and evaluation options may be applied by the bank at any time, provided these do not result in any changes in the use of data (see Sections 10a.3 and 10a.4). The Bank will inform the customer about any such changes within online banking.

11 NOTIFICATION SERVICE

11.1 The customer can register in online banking for the Bank's free notification service. When the customer registers for the notification service, the customer-specific data and information specifically selected by the customer during the registration (e.g. notification of a completed PIN change, notification of login attempts with an invalid PIN, notification if the balance goes above/below a limit specified by the customer) are transmitted to the e-mail address specified by the customer or another communication channel agreed with the customer.

11.2 The customer may activate or deactivate the notification service at any time in online banking. The customer may change the order data (e-mail address or another communication channel as well as events that trigger a notification to the customer) at any time. A valid TAN or the ATC is required for the activation or deactivation of the notification service and for the change in the order data.

11.3 Termination of the agreement to participate in online banking (OnlineBanking or 24You) that the customer has concluded with the Bank ends the notification service automatically. The Bank may terminate the free notification service in compliance with a notice period of two months without giving reasons.

12 AMENDMENTS TO THE TERMS AND CONDITIONS

12.1 Changes to these Terms and Conditions shall be offered to the customer by the Bank not later than two months before the proposed date of their coming into effect, with the Bank specifically referring to the relevant provisions. The customer shall be deemed to have consented to the changes unless the Bank receives an objection to the changes from the customer before the proposed date of their coming into effect. The Bank shall draw the customer's attention to this fact in its offer of changes. The offer of changes shall be provided to the customer.
Moreover, the Bank will publish on its website a comparison of the provisions affected by the changes to the Terms and Conditions and the complete version of the new Terms and Conditions, and provide the customer with these Terms and Conditions at his/her request in written form at its branches or by sending them to the customer by regular mail. In its offer of the changes, the Bank shall draw the customer's attention to this option.

12.1a The notification regarding the change offered in accordance with Section 12.1 is made either by post to the last address provided by the customer (see also Section 11 Para. 2 of the Bank's General Terms and Conditions) or in electronic form via the online banking mailbox. This electronic notification shall be made in such a way that the Bank can no longer modify the offer of changes unilaterally and the customer may

save and print the notification. If such an electronic notification is made via online banking, the Bank will simultaneously inform the customer that the offer of changes is available and retrievable in his/her online banking mailbox. This is done by sending a separate e-mail to the last e-mail address provided by the customer or a separate SMS to the mobile phone number originally provided by the customer for receiving SMS in the context of online banking.

12.1b Vis-à-vis an entrepreneur it is sufficient to send the offer of changes to the online banking mailbox or make it available in some other way agreed with the entrepreneur not later than two months prior to the proposed date of the entry into force of the changes.

12.2 In the event of such intended changes to the Terms and Conditions, a customer who is a consumer shall have the right to terminate his or her master agreements on payment services, and in particular this Agreement or the current account maintenance agreement, free of charge and without giving notice, before such changes come into effect. The Bank shall draw the customer's attention to this fact in its offer of changes.

12.3. Sections 12.1 to 12.2 above will also apply to changes to the Agreement in accordance with Section 1.2 in which the application of these Terms and Conditions has been agreed between the customer and the Bank.

12.4. Paragraphs 12.1 to 12.3 above do not apply to changes in the Bank's services and in charges payable by the customer.

B SPECIAL CONDITIONS FOR THE SECURITIES FUNCTION

1 GENERAL INFORMATION

Online banking enables the customer to purchase and sell equities, warrants, bonds, exchange traded funds, index certificates on selected exchanges as well as domestic and foreign funds selected by the Bank and registered for sale in Austria, and to subscribe to selected new issues.
The exchanges on which users can currently effect securities transactions via online banking and the types of securities that can be traded on the relevant exchanges via online banking are listed in the "Terms and Conditions for Securities Trading via the Internet and SmartBanking at a Glance". These are available on www.bankaustria.at and upon request at any of the Bank's branches.

2 PLACING ORDERS AND SERVICE HOURS

2.1 Orders can be placed via online banking 24 hours a day, 7 days a week (see Part A, Section 4.1).

2.2 In this way, purchase and sale orders for individual securities positions can be placed on a same-day basis (intraday trading) in online banking.

2.3 The customer is provided with customer information documents (Key Information Documents – KID) as defined in the Austrian Investment Fund Act (Investmentfondsgesetz), which can be accessed in the online banking portal (access via online.bankaustria.at or banking.bankaustria.at /Investment & Market Info / Securities Finder /Securities Finder - Global entering the fund ISIN and then clicking the "KID button" in the results line). The customer and the Bank agree that the Bank will make available to the customer, via online banking, key information documents pursuant to the "Regulation on key information documents for packaged retail and insurance-based investment products (BIB)". The customer has the right to demand a free paper copy of KID and BIB.

2.4 The sale of pledged securities, or securities to be treated by the Bank as blocked securities for any other reason, that are held in the specified securities account(s) is not possible in online banking.

2.5 The Bank will provide the customer with legally binding confirmation of the execution of the orders placed and the settlement note in writing via the agreed method for sending account correspondence. Therefore, an electronic order confirmation is only considered confirmation of the Bank's acceptance of the order for processing but not confirmation of execution or settlement.

2.6 Placing a purchase order via online banking is only permitted if – at the time the order is placed – the settlement account selected for the purchase order has the necessary cover (credit balance or agreed overdraft facility) for the execution of the order.

2.7 The customer is responsible for obtaining information on the trading hours at the time the order is placed and on standard practices of the relevant exchange. The Bank assumes no liability for damage or losses sustained by a customer because his/her order placed via online banking does not comply with the trading practices of the desired exchange.

3 LIEN

The securities posted to the securities account(s) specified for online banking, as well as interest income and proceeds from redemption or sale of such securities, are subject to the lien defined in Section 49 ff. of the General Terms and Conditions of UniCredit Bank Austria AG for all receivables to which the Bank is entitled under the business relationship. If the prices of the values deposited on the dedicated securities account(s) decrease to such an extent that a liability on the associated clearing account is no longer covered, the customer undertakes, as a current or securities account holder to either hand over further securities in the corresponding amount to the Bank by way of a

pledge, or to cover the exposure to the extent that sufficient collateralisation is restored. Coverage values not required within the framework of this lien remain at the customer's discretion in agreement with the Bank in consultation with the respective Customer Account Manager. The Bank expressly declares the right to block security account funds in connection with the lien if this is necessary to ensure receivables from the management of securities or from the other business relationship. The Bank is entitled to sell the pledged securities or those which are subject to the block on securities as defined by the General Terms and Conditions of UniCredit Bank Austria AG in whole or in part if the above-mentioned variation margin or coverage is not provided or a claim asserted by the business relationship (in particular also from the management of securities) is not settled in a timely manner.

ANNEX TO THE TERMS AND CONDITIONS FOR ONLINE BANKING

Recommendation of Bank Austria for security on the Internet and use of online banking:

1 The online banking system communicates over the Internet. The Internet is an open and publicly accessible communication medium. An unauthorised person could use the personal identification details of a customer to gain access to the online banking system and effect transactions to the debit of the customer's current/securities account. Bank Austria regularly provides information, on the Bank's security portal https://sicherheit.bankaustria.at and directly in the online banking system, on current potential threats in the Internet as well as making specific security recommendations and suggestions for ways in which a customer can adjust his/her behaviour when using online banking services so as to minimise risk associated with potential threats in the Internet. Customers are strongly advised to exercise particular caution when conducting transactions via online banking to prevent any damage or losses.

2 Bank Austria employs comprehensive measures to secure the data transmitted via online banking and the data processed at the Bank and employs comprehensive security measures to protect data against attack when they are transmitted via the Internet or processed on the Bank's servers. In order to ensure that the security measures are as effective as possible, the Bank also recommends every customer to take technical measures to protect his/her own computers and data processing systems in his/her own interest. The Bank provides information on potential threats and suitable security measures for protecting the customer's data processing systems and computers on its website and in the online banking system.