Schoellerbank
Private Banking

General Terms and Conditions of Electronic Banking of Schoellerbank AG

Schoellerbank Electronic Banking (Schoellerbank Online Banking, Schoellerbank Business Banking, and the Multi Bank Standard Service [MBS Service]) allows banking transactions, in particular payment and securities orders and account balance and portfolio holdings queries, to be performed for specifically defined accounts. The scope of services can differ depending on the specific bank product.

A Internet Banking

1. General

1.1 Internet banking (Schoellerbank Online Banking) is a special service offered by Schoellerbank AG (called the "Bank" in the following) that enables a customer as a (securities) account holder or authorised signatory to establish communication with the bank data processing centre via data transmission over the Internet and to call up information about accounts and submit orders to be completed through (securities) accounts after proper electronic authorisation.

Internet banking also offers a version that is optimised for use through mobile devices (such as smartphones and tablets).

1.2 The "Online Banking Application" or "Online Banking Application with Securities Account Access" (called the "Agreement" in the following) is concluded between the Customer and the Bank for an open-ended period and authorises the Customer to make use of Internet banking. This confers to the Customer Internet banking authorisation for all (securities) accounts of which he/she is the holder. The (securities) account holder must grant written authorisation to allow authorised signatories to access the account in question through Internet banking. For joint (securities) accounts, all account holders must authorise Internet banking access for an individual account holder or authorised signatory.

If collective signatory powers are agreed for a securities account, no orders can be submitted through Internet banking, and the Internet banking access to these securities accounts is limited to calling up account information. If collective signatory powers are agreed for a non-securities account, Customers can only execute a transaction together with all other authorised persons.

An order that has been signed by only one user with collective signing authority using his/her TAN will be irrevocably cancelled in the system without being executed and without further account information being provided by the Bank if it is not signed by a second user with collective signing authority using his/her TAN within 28 days.

2. Definitions

2.1 Personal user name (user identification)

Each Customer is assigned a unique, multi-character personal user name by means of which the Bank can uniquely identify the Customer. The personal user name is given to the Customer when the Agreement is signed. The Customer can change his/her personal user name.

PC282E - 023GI9210E 20200101

2.2 Password (personal identification number)

The Bank will provide the Customer with a password that the Customer must then change the first time he or she logs into Internet banking. Every time the Customer logs into Internet banking after this, he/she must provide the correct personal user name, the defined password, and the second authentication factor (e.g. cardTAN). The Customer will receive the password in a sealed envelope either in person upon signing the Agreement or by regular mail. The Customer can change his/her password at any time in Internet banking using a TAN. The changed password must be used every time the Customer logs into Internet banking. For security reasons, the Bank can require the Customer to change the password to a password with a greater number of characters or a higher degree of complexity. The Customer can request a new password in person at any branch of the Bank during regular business hours. The new password will be given to the Customer in the selected branch of the Bank or sent to the Customer by regular mail.

2.3 shortPIN

The service can also be accessed on mobile devices using simplified authentication (device integration combined with a user-specific four-digit PIN code).

2.4 FIDO token (login method)

The FIDO token (a hardware unit with a USB plug) can be purchased from retailers and enables the Customer to authenticate himself or herself for the purposes of logging into Internet banking. To do this, the Customer must plug the FIDO token into a USB port on his/her device and confirm the authentication procedure.

2.5 Transaction number (TAN)

A TAN is an authentication code that is generated for a specific instance and is used for logging into Internet banking (in addition to the personal user name and password) and for submitting orders and other legally binding declarations of intent to the Bank through Internet banking.
Once the TAN is entered in the corresponding box and confirmed by means of the corresponding button, the order or declaration of intent is officially submitted.
The Bank offers the Customer different TAN methods for use in Internet banking. Should the Bank be unable to continue offering a TAN method that is used by the Customer because

- objective concerns pertaining to the security of this TAN method or the systems for which it is used justify its discontinuation, or
- the Bank is no longer permitted to offer the TAN method that is used by the Customer for legal or supervisory reasons, the Bank shall inform the Customer of the reasons for this and, if the Customer is not prepared to use a different TAN method that has been enabled for him/her and that employs a higher security standard, will offer the Customer the switch to a different TAN method with a higher security standard free of charge. The Bank shall submit this offer to the Customer via the method agreed for the submission of notices under the business relationship in good time so that the Customer receives this offer by no later than two months before the proposed time of the switch. This offer shall be considered to have been accepted by the Customer if no objection from the Customer has been received by the Bank before the proposed time of the switch. In this notice, the Bank shall inform the Customer of the consequences of failure to submit a response and of the Customer's right to termination free of charge according to item 11.3.
- If the Customer refuses the Bank's offer by submitting an objection and chooses to exercise his/her right of termination, the personal user name will be blocked. If the Customer refuses the offer to switch to a different TAN method with a higher security standard, the TAN method used by the Customer shall be discontinued no earlier than two months after the offer to switch is sent. Despite having objected, the Customer shall be entitled to switch to the offered TAN method with a higher security standard at any time up to the point in time at which the TAN method used by the Customer is discontinued. The Customer can inform the Bank of his/her desire to switch to the offered TAN method in person at a branch of the Bank, by telephone, or by regular mail.

PC282E - 023GI9210E 20200101

a) mobileTAN

If the Customer wishes to use the mobileTAN method, he/she can inform the Bank of this in person at a branch of the Bank, by telephone, or by regular mail. If the Customer uses the mobileTAN method, the mobileTANs needed to log into Internet banking, sign previously created Internet banking transactions, and submit declarations of intent will be sent to a mobile device (e.g. mobile telephone or tablet) via text message.

The Customer must provide the number of the mobile phone that is to be used for the text messages sent for the mobileTAN method in person at a branch of the Bank before the mobileTAN method is used for the first time. The Customer can change the mobile phone number provided for the receipt of text messages in person at a branch of the Bank, or in Internet banking using a mobileTAN provided that the Bank can send a text message to the Customer at the mobile phone number currently on file with the Bank.

The Bank can suspend the ability to change the mobile phone number and to change the method for the provision of mobileTANs via Internet banking for security reasons if this is justified by objective reasons relating to the security of the personal identifiers or the systems for which they can be used. The message containing the mobileTAN also contains information about the transaction to be completed (especially for payment transactions: International Bank Account Number [IBAN] or payee account number, Bank Identifier Code [BIC] or sort code of the payee's bank, and the amount to be transferred) for verification purposes.

A mobileTAN can only be used to execute the transaction for which it was requested. If a transfer order is changed after a mobileTAN is issued for it, the previously issued mobileTAN will be invalidated and a new mobileTAN must be requested. A mobileTAN is rendered invalid once it is used. When using the mobileTAN method, the Customer is obligated to check the verification data sent in the message with the mobileTAN (e.g. the IBAN of the payee account, payment amount) to ensure that it matches the submitted order and must only enter the mobileTAN together with his/her password if the order data match.

Delivery of mobileTANs by text message: The Customer can only receive a text message with a mobileTAN on his/her mobile phone if the requirements for text message receipt are met, for example:

- the telephone is capable of receiving text messages,
- the contract with the mobile communications provider includes the receipt of text messages, and
- the Customer is in an area where his/her mobile communications provider delivers text messages.

b) Schoellerbank ID app

The Schoellerbank ID app is an application for (mobile) devices and allows for Customer authentication. To authenticate himself or herself, the Customer is shown a number in the Internet banking system. At the same time, a series of numbers is shown to the Customer in the Schoellerbank ID app together with the specific case requiring authentication (e.g. details about a payment order). To complete the authentication procedure, the Customer must select the number that is also shown in Internet banking (by touching the number).

Each device on which the app is installed must be assigned to the Customer after installation by means of the device integration process. Authentication is completed by means of the device integration and shortPIN or a biometric method (fingerprint or FaceID). The user can change his/her device integration and shortPIN directly in Internet banking.

Information on the transaction to be completed (the payee's IBAN and amount or a reference code [electronic note] and control value [total amount of all orders]) will also be shown during the authentication process for verification purposes. The Customer is required to check that this information matches the orders entered in Internet banking. Authorisation may only be given if the information matches.

PC282E - 023GI9210E 20200101

The Customer can only receive a number from the Schoellerbank ID app on a mobile device such as a smartphone or tablet if the following requirements are met:

- the Customer has a current version of the Bank Internet banking app (Schoellerbank ID app) installed,
- the Customer is in an area where his/her mobile communications provider or a WiFi network provides an Internet connection.

c) cardTAN

If the Customer wishes to use the cardTAN method, he or she must inform the Bank of this in person at a branch of the Bank, by telephone, or by regular mail.

The Customer needs a special card reader (cardTAN generator), an active (i.e. neither blocked nor expired) cardTAN-compatible card (debit card or TANcard), and an electronic banking PIN in order to use the cardTAN method.

The Customer can request a cardTAN generator directly at the Bank. After the cardTAN-compatible card (debit card or TANcard) is inserted into the cardTAN generator and the electronic banking PIN is entered, the data for the login into Internet banking or the transaction to be signed are entered into the cardTAN generator via an optical interface (see "flicker" mode) or manually by the user. Then, a cardTAN is generated via a special program stored on the chip of the debit card or TANcard. The Customer must enter the cardTAN in Internet banking, after which it is verified by the Bank. The cardTAN generator can be used in "flicker" mode or "manual entry" mode. "Flicker" mode is the simpler method, but if there are problems with data transmission via the flicker code, the Customer can switch to "Manual entry on the cardTAN generator" in Internet banking. "Flicker" mode: The data needed to calculate the cardTAN, especially the transaction data, are transmitted to the cardTAN generator by the bank server by means of a black and white blinking optical interface on the Customer's screen (e.g. computer or tablet). The transaction data representing the transaction to be authorised by the Customer are shown on the display of the cardTAN generator so that the Customer can verify them. When using the cardTAN method with "flicker" mode, the Customer is obligated to check the presented verification data (e.g. the IBAN of the payee account, payment amount) to ensure that it matches the submitted order and must only use the cardTAN if the transaction data match.

"Manual entry" mode: For this, certain data requested on the Internet banking screen, especially the transaction data, must be entered by the Customer into the cardTAN generator. When using "manual entry" mode, the Customer is obligated to verify that the entered transaction data match his/her order and must only use the cardTAN if the transaction data match.

A cardTAN can only be used to execute the transaction for which it was generated. If a transfer order is changed after a cardTAN is generated for it, the previously generated cardTAN will be invalidated and a new cardTAN must be generated using the cardTAN generator. A cardTAN is rendered invalid once it is used.

2.6 Biometric data

When using the Bank's Internet banking apps on mobile devices (smartphones or tablets), the Customer can connect the password with biometric data (such as a fingerprint or FaceID) in the respective Internet banking app if the device being used supports such functionality. In this case, the Customer will be verified on the basis of his/her biometric data saved in the Internet banking app instead of entering a password when logging into mobile Internet banking.

2.7 Personal identifiers

The user name, password, transaction numbers (TAN), and biometric data saved in the Bank's Internet banking apps represent the personal identifiers of the Customer.

3. Authenication

The Bank verifies the Customer's authorisation to use Internet banking on the basis of the entered personal identifiers.

PC282E - 023GI9210E 20200101

4. Transaction through Internet banking

4.1 Account transactions and declarations of intent (collectively called “transactions” in the following) can generally be submitted to the Bank through Internet banking 24 hours per day and 7 days per week. In the event that maintenance work must be completed on the Bank’s servers, a maintenance window is scheduled between 00:00 and 6:00. During this time, Internet banking may be unavailable when such maintenance work is being conducted. If maintenance work has to be performed between 06:00 and 24:00, Schoellerbank will inform Customers in advance if possible.

4.2 The Customer establishes a connection with the Bank’s server by logging into Internet banking through the website by entering his/her user name and password and using the respective login authentication method.

The Customer must enter the information required for the desired transaction on the screen and then submit the order via data transmission over the Internet. The Customer must always enter the customer identifier of the payee when entering transfer orders. If the Customer provides information about the payee beyond this, such as the payee’s name or purpose of the payment, such information is not part of the customer identifier and therefore shall only serve for documentation purposes and will be disregarded by the Bank in the execution of the transaction. The Customer must then conclude the desired transaction by entering the TAN generated for the transaction in question and pressing the button intended for authorisation.

4.3 The time that a transaction is received by the Bank via Internet banking shall be considered the time of receipt. If a transaction submitted through Internet banking is received on a day that is not a business day of the Bank or after a certain time close to the end of a business day, this transaction will be treated as if it had been received on the next business day. The Bank publishes these times in the “Information about Payment Transaction Services for Consumers at Schoellerbank AG”, which can be obtained electronically from the website or in printed form upon request from the Bank’s branches or by regular mail.

The Customer can also specify that an order be executed on a date in the future (scheduled order). If the desired execution date for a scheduled order is not a business day of the Bank, the order will be treated as if it had been received on the following bank business day.

4.4 As many transfer orders as desired can be submitted for an account through Internet banking. The Bank shall only be obligated to execute a transfer order if sufficient cover for the full amount is available in the Customer’s account. The Customer can also combine multiple transfer orders and sign them with a single TAN.

4.5 General information about limits with the mobileTAN, Schoellerbank ID, and cardTAN methods:

4.5.1 Transaction limits can be set for Internet banking.
The transaction limit sets the maximum amount of a single transfer order or the maximum amount for the total of multiple transfer orders that can be signed with a single TAN.

4.5.2 A limit can be set unilaterally by the Bank (see item 4.5.3) or can be agreed between the Bank and Customer. In both cases, this is a “bank limit”.

4.5.3 The Bank is entitled to apply or reduce a bank limit without consulting the Customer if

- there are objective grounds to do so with regard to the security of the personal identifiers or the systems for which they can be used, or
- there is reason to believe that unauthorised orders have been submitted using the personal identifiers, or that the personal identifiers have been misused in some other way. The Bank will inform the Customer of such a bank limit (reduction) before it is enacted if possible, or immediately after it is enacted through the agreed communication channel, including the reason for this limit (reduction).

PC282E - 023GI9210E 20200101

4.6 An authorised transfer order submitted to the Bank via Internet banking cannot be cancelled. A scheduled order that has been submitted to the Bank can be cancelled up until the end of the business day before the agreed execution date directly in Internet banking using a valid TAN.

4.7 eps online transfer

Internet banking can also be used to execute eps online transfers. The eps online transfer is a standardised payment process for online purchases and for the use of e-government services. If the website of the Internet shop or the e-government website displays the logo for eps (e-payment standard) and online transfers, the Customer can use his/her personal user name, password, and the selected login authentication method to log directly into Internet banking and make the payment by means of a transfer order. An eps online transfer is authorised in the same manner as every other transfer in Internet banking using a TAN (see item 4.2). None of the Customer's bank-specific data are accessed or stored by a third party at any point during the eps online transfer procedure because the Customer logs directly into Internet banking through the Bank's website or in the Bank's banking app and authorises the transaction there. The Bank also transmits no bank-specific data of the Customer during the execution of an eps online transfer. When the eps online transfer is signed by the Customer, the Bank guarantees the execution of the transfer to the online merchant or e-government authority, meaning that the Customer cannot cancel this eps online transfer. The eps online transfer process is merely a tool that the Customer can use to make an online payment by way of a transfer order in Internet banking. The contractual relationship between the Customer and the merchant is not affected by the use of the eps online transfer process, and therefore no objections relating to the underlying transaction may be asserted against the Bank.

5. Account information service providers and payment initiation service providers

5.1 The Customer may allow account information service providers and payment initiation service providers to access one or more of his/her payment accounts that can be accessed through Internet banking by making use of the services of these providers.

5.2 Account information service providers offer consolidated information about one or more payment accounts of an account holder, including accounts at different banks. Payment initiation service providers initiate a payment transaction from a different payment account when requested to do so by the account holder, including accounts at different banks.

5.3 If the Customer employs an account information service provider or payment initiation service provider by allowing these service providers to access one or more of his/her payment accounts, the Bank is obligated under Delegated Regulation (EU) 2018/389 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication to communicate with these service providers in a secure manner and to provide them with the authentication methods required to verify the identity of the Customer.

6. Due diligence

6.1 The Customer is obligated in his/her own interests to keep his/her password and TAN in strict confidence and not disclose them to other persons (including not to employees of the Bank). The storing of a biometric password (see item 2.6) does not relieve the Customer from his/her duty to keep the password and TAN in strict confidence. The prohibition on disclosing the password or TAN does not apply to account information service providers or payment initiation service providers that are employed by the Customer. The Customer must immediately change his/her password should there be reason to believe that another person has learned his/her password or that his/her Internet banking access has been used by an unauthorised person. For security reasons, the Customer is advised to change his/her password regularly (e.g. every three months). The Customer must immediately report any unauthorised use of his/her Internet banking access to the Internet banking hotline (see item 8.1). The Customer is advised to have his/her mobile phone to which mobileTANs are sent blocked immediately in the event of theft or loss.

PC282E - 023GI9210E 20200101

6.2 If the URL accessed to log into Internet banking does not start with https://banking.schoellerbank.at/ or if the web browser does not display the padlock icon for encrypted data transfer, these are indications that the Customer is not on the Bank's website. The Customer may be using a website set up for the purpose of obtaining the Customer's personal identifiers by means of phishing. In this case, the Customer is advised to abort the login procedure and to immediately contact the Internet banking hotline (see item 8.1.) if any personal identifiers were entered on the website in question.

6.3 When using the mobileTAN method or Schoellerbank ID app, the Customer is obligated to check the verification data sent in the message with the mobileTAN or shown in the Schoellerbank ID app (e.g. the IBAN of the payee account, payment amount) to ensure that it matches the submitted order and must only use the mobileTAN or the number shown in the Schoellerbank ID app if the order data match. When using the cardTAN method with "flicker" mode, the Customer is obligated to check the presented verification data (e.g. the IBAN of the payee account, payment amount) to ensure that it matches the submitted order and must only use the cardTAN if the transaction data match. When using the cardTAN method with "manual entry" mode, the Customer is obligated to verify that the transaction data entered in the cardTAN generator match his/her order as entered in Internet banking and must only use the generated cardTAN if the transaction data match.

6.4 When using Internet banking, the Customer is obligated to comply with the provisions of these terms and conditions of use, and in particular to enter the customer identifier correctly when submitting orders (see item 4.2) and to only submit a transfer order when sufficient coverage is available on the account from which the transfer order is to be debited.

7. Correction of unauthorised payment transactions

In the event of an account debit as a result of an unauthorised or incorrectly executed payment transaction, the Customer is entitled to have the transaction corrected by the Bank if the Bank is informed of the unauthorised or incorrect transaction immediately, in any case by no later than 13 months after the date of the debit, unless the Bank failed to inform the Customer of the transfer order or payment debited from his/her account (reference, amount, currency, fees, interest, exchange rate, value date of the debit) in the agreed manner or failed to make this information available in the agreed manner. This does not preclude any of the Customer's other rights to correction. In the event of an unauthorised payment transaction, the Bank shall reimburse the Customer for the amount of the unauthorised payment transaction immediately, but in any case at the latest by the end of the next business day after it becomes aware of or is notified of the payment transaction. The reimbursement shall be effected by restoring the debited account to the balance that would have existed without the unauthorised payment transaction. The amount shall be booked to the payer's payment account with a value date corresponding to the date of the debit at the latest. If the Bank has notified the Financial Market Authority in writing of reasonable grounds for suspicion that the Customer engaged in fraudulent conduct, the Bank must review the matter and meet its reimbursement obligation immediately if the suspicion of fraud proves to be unwarranted. The Bank is also obligated to reimburse the Customer for an unauthorised payment transaction if it was initiated by a payment initiation service provider.

8. Blocking

8.1 Every (securities) account holder and every authorised signatory can block his/her personal user name as follows:

- at any time by telephone through the Bank's Internet banking hotline, whose number can be found on the website www.schoellerbank.at, or
- in person or in writing at any branch of the Bank during regular business hours. A block request submitted to the Bank during regular business hours or through the Internet banking hotline at any time of the day will take effect immediately after receipt of the block request. Written block requests received by the Bank outside of its business hours will take effect immediately after the start of the next business hours, or
- at any time in Internet banking under the menu Security / Blocking.

PC282E - 023GI9210E 20200101

8.2 The Bank shall be authorised to block a personal user name without the Customer's involvement if

- there are objective grounds to do so with regard to the security of the personal identifiers or the systems for which they can be used, or
- there is reason to believe that unauthorised orders have been submitted using the personal identifiers, or that the personal identifiers have been misused in some other way. The Bank will inform the Customer of the block and also the reasons (when this is not in violation of Austrian or Community regulations, a court or other legal order, or objective security concerns) in the form agreed with the Customer before the block is enacted if possible, or immediately after the block is enacted.

8.3 The access to Internet banking will be temporary blocked after the personal code is entered incorrectly three times. Additional incorrect entries increase the duration of the temporary blocking of the user's access as shown below:

- after the 3rd incorrect entry: 30 seconds wait until the next attempt
- after the 5th incorrect entry: 2 minutes wait until the next attempt
- after the 7th incorrect entry: 10 minutes wait until the next attempt
- after the 10th incorrect entry: 1 hour wait until the next attempt

Once the personal code is entered correctly one time, access to Internet banking is restored.

8.4 The Customer can personally request that the block be lifted through any communication channel agreed with the Bank (in particular through the Customer's relationship manager or at any of the Bank's branches).

8.5 The Bank shall be entitled to deny access to an Internet banking-enabled payment account of the Customer by a payment initiation service provider or an account information service provider if this is justified by objective and duly verified reasons in connection with unauthorised or fraudulent access to the payment account on the part of the payment initiation service provider or the account information service provider, including the unauthorised or fraudulent initiation of a payment transaction. The Bank will inform the Customer if access to a payment account of the Customer by a payment initiation service provider or an account information service provider is blocked and also the reasons – provided that this is not in violation of a court or other legal order, Austrian or Community law, or objective security concerns – using a communication method agreed with the Customer before the block is enacted if possible, or at the latest immediately after the block is enacted.

9. Expiration and termination of access

9.1 When an account is terminated, all Internet banking authorisations for the account expire automatically. If sole signatory powers of a (securities) account holder or an authorised signatory for a (securities) account are rescinded, access to this account through Internet banking will be revoked.

9.2 Every Customer can terminate the Agreement in writing at any time with a period of notice of one month. Every (securities) account holder may revoke the Internet banking authorisation of an authorised signatory in writing or in person at any of the Bank's branch offices.

9.3 The Bank can terminate the Agreement at any time without justification in writing with a period of notice of two months. In this case, the (securities) account holder must be informed of the termination in writing or by means of any other agreed durable data medium.

9.4 The Agreement can be terminated immediately without a period of notice by the Customer or the Bank for good cause. Good cause shall be deemed to exist if the Customer makes his/her personal identifiers available to another person.

PC282E - 023GI9210E 20200101

10. Notification service

10.1 The Customer can sign up for the Bank's free notification service in Internet banking. If the Customer signs up for the notification service in the communication settings, the customer-related data and information (such as notification when the Customer's account balance falls below or above a certain limit, security price alarms, etc.) specifically selected by the Customer will be sent to the e-mail address indicated by the Customer or through another communication channel agreed with the Customer.

10.2 The Customer can activate and deactivate the notification service in Internet banking at any time. The communication settings (communication channel and events that trigger a notification to the Customer) can be changed by the Customer at any time.

11. Amendments to the terms and conditions

11.1 Amendments to these terms and conditions will be proposed to the Customer by the Bank, with reference to the affected provisions, at least two months before the proposed date of the entry into force of such amendments. If the Bank has received no objections from the Customer by the proposed date of the entry into force, this shall represent tacit acceptance on the part of the Customer. The Bank shall inform the Customer of this fact in the amendment proposal. The Customer shall be informed of the amendment proposal. The Bank shall also publish a comparative overview of the provisions of the terms and conditions that are to be amended as well as the complete version of the new terms and conditions on its website, and shall provide this information to the Customer in printed form at its offices or by regular mail upon request. The Bank shall inform the Customer of these options in the notice regarding the proposed amendments.

11.1a The notice regarding the proposed amendments according to item 11.1 shall be sent by regular mail to the last known address of the Customer (see also section 11 [2] of the General Terms and Conditions of the Bank) or in electronic form via "Notifications" in Internet banking. This electronic notice shall be made in such a way that the Bank can no longer make unilateral changes to the amendment proposal and the Customer can save and print out the notice. If such electronic notice is submitted via the Internet banking platform, the Bank shall inform the Customer that the amendment proposal is available and can be accessed via "Notifications" in Internet banking. This shall be communicated by sending a separate e-mail to the e-mail address most recently advised to the Bank by the Customer or through another communication channel agreed with the Customer.

11.1b If the Customer is an entrepreneur, it shall be sufficient to make the amendment proposal available for access by the Customer via "Notifications" in Internet banking or in another form agreed with the Customer at least two months before the proposed date of the entry into force of the amendments.

11.2 In the event that amendments to the terms and conditions are planned, Customers who are consumers shall be entitled to terminate their framework agreements for payment transaction services, particularly this Agreement or the current account agreement, with no period of notice and at no cost before the amendments take effect. The Bank shall include notice of this fact in the amendment proposal.

11.3 Items 11.1 to 11.2 also apply to amendments to the Agreement according to item 1.2, which governs the applicability of this business relationship between the Customer and Bank.

11.4 The previous items 11.1 to 11.3 shall not apply to changes to the services of the Bank and the fees charged to the Customer.

PC282E - 023GI9210E 20200101

B Special terms for the securities function

1. General

Shares, warrants, bonds, index certificates on selected exchanges, and selected domestic and foreign funds that are sold by the Bank can be purchased and sold through Internet banking. The current exchanges on which the Customer can trade through Internet banking and the types of securities that can be traded through Internet banking on the eligible exchanges can be found in the best execution policy. This information can also be obtained on the Bank's website www.schoellerbank.at or at any of the Bank's branches.

2. Order placement and usage times

2.1 Orders can generally be placed through Internet banking 24 hours a day and 7 days a week (see section A, item 4.1).

2.2 In this way, buy and sell orders for individual securities positions can also be placed for the same day (intraday trading) through Internet banking.

2.3 The sale of pledged securities or other positions in the respective securities account that are to be held by the Bank as blocked for some other reason is not possible through Internet banking.

2.4 The Bank shall submit to the Customer legally binding confirmations of the execution of the placed orders and of order settlement in the manner agreed for account correspondence. An electronic order confirmation is thus simply the confirmation of the receipt of the order by the Bank for processing, but is not a confirmation of execution or settlement.

2.5 A purchase order can only be submitted through Internet banking if the settlement account selected for the buy order has sufficient coverage (credit balance or agreed overdraft facility) for the execution of the order at the time that the order is placed.

2.6 The Customer must inform himself/herself of the trading times and practices on the respective exchange at the time that the order is submitted. The Bank shall not be liable for damages incurred by the Customer due to orders submitted through Internet banking not conforming with the trading practices on the selected exchange. If the electronic securities order placed by the Customer without prior consultation does not correspond to his/her knowledge and experience in the investment field, Schoellerbank shall be entitled to refuse execution.

3. Liens

All securities posted to the securities account(s) that can be accessed through Internet banking and all associated interest, redemption, and sales proceeds shall be subject to the right of lien according to section 49 ff. of the General Terms and Conditions of Schoellerbank AG in relation to all claims of the Bank arising from the business relationship. Should the prices of the securities posted to the respective securities account decline so far as to not cover outstanding claims against the associated settlement account(s), the Customer as (securities) account holder shall either pledge to the Bank additional securities that are acceptable as collateral to the Bank or shall satisfy the outstanding claims to the extent required to ensure sufficient collateral coverage from the securities in the securities account in question within the time period set by the Bank. Assets not required under this right of lien shall be at the free disposal of the Customer in agreement with the Bank and in coordination with the Customer's relationship manager. The Bank expressly reserves the right to place a lien on securities in the account to the extent necessary to secure claims from the management of the securities account or from other aspects of the business relationship. The Bank shall be entitled to sell part or all of the securities pledged or subject to the securities account block as defined in the General Terms and Conditions of Schoellerbank AG if the Customer does not meet the coverage requirement set forth above or fails to satisfy a claim of the Bank arising from the business relationship (especially from securities account management) in good time.

PC282E - 023GI9210E 20200101

C Special terms for Schoellerbank Business Banking and the Multi Bank Standard Service (MBS Service)

These special terms also apply to entrepreneurs.

The products Schoellerbank Business Banking (HBP) and Multi Bank Standard Service (MBS Service) are subject to section A of these terms and conditions as follows: Authentication can be effected via mobileTAN or cardTAN (item 2.5.a and 2.5.c). The items 6 (Due diligence), 7 (Correction of unauthorised payment transactions), 8 (Blocking), 9 (Expiration and termination of access), and 11 (Amendments to the terms and conditions) also apply. The other provisions do not apply to the following bank products.

1. Schoellerbank Business Banking (HBP)

1.1 Access to Schoellerbank Business Banking

User number: The Customer shall receive a user number from Schoellerbank AG by regular mail, which enables Schoellerbank AG to assign a Customer to the accounts which he is authorised to access via Schoellerbank Business Banking. It consists of a multi-digit code that is generated by the system when it is issued. The user number may not be changed by the Customer.

Bank user name: The bank user name must be created by the Customer the first time he or she logs into Schoellerbank Business Banking. The bank user name can be changed at any time and with immediate effect using a TAN.

Password (PIN/personal identification number): The password serves to verify the Customer's identity in the Electronic Banking system and must be entered before the Customer can submit orders and access information through Schoellerbank Business Banking. The PIN is a 16-character alphanumeric code. This initial PIN must be changed by the Customer the first time he/she logs into the selected Electronic Banking product. The PIN can be changed at any time and with immediate effect using a TAN. The Customer can request a new initial PIN by contacting his/her relationship manager by phone.

1.2 Procedures

In addition to the personal access credentials described in item 1.1., the following must be defined by every authorised user in Schoellerbank Business Banking:
Personal user name (user identification for logging into Schoellerbank Business Banking) and password (can be changed by the authorised user at any time). In Schoellerbank Business Banking, the personal user name and password are locally stored access credentials used to log into the program and are not the personal access credentials described in item 1.1. These features are intended to ensure the internal security of the Customer and are independent from the personal access credentials assigned by the Bank.

1.3 Prerequisites for access

Authorisation to use Schoellerbank Business Banking is conferred through the usage agreement "Application for the Use of Schoellerbank Business Banking". The Customer will receive his/her access credentials (user number and personal identification number) for Schoellerbank Business Banking by regular mail or personal letter. Communication can only be established when the credentials assigned by the Bank (user number and PIN) and defined by the Customer (personal user name) are entered correctly. The PIN assigned by the Bank must be changed during the first login.

PC282E - 023GI9210E 20200101

The object of the Agreement is the acquisition of the single, non-transferrable right to use the Schoellerbank Business Banking software product as well its use for the (securities) accounts managed by Schoellerbank AG to the extent agreed. Schoellerbank Business Banking essentially corresponds to the “Multi Bank Standard”, which allows the Customer to manage all Austrian bank accounts that support MBS using a single software product. The Customer is not permitted to copy the Schoellerbank Business Banking software or share it with third parties. The creation of a back-up copy to facilitate operational security is excepted from this rule. The Bank expressly retains ownership of the intellectual property comprising the software and documentation and all associated rights. The Bank provides no guarantee of the proper functionality of the software. The installation and use of the software occur at the user’s own risk.

1.4 Updates and technical modifications

The Bank may implement updates and modifications to the data transmission functionality or user interface at any time in line with technical progress and additional security measures. Any software modifications and enhancements will be transferred automatically during communication with Schoellerbank AG. The Customer is obligated to ensure the proper installation of software updates. The Bank may also extend the scope of the features available in Electronic Banking, provided that this does not result in additional costs or obligations for the Customer.

In order to use Schoellerbank Business Banking, the Customer must ensure that unrestricted data transfer via the URL hob.banking.co.at is not impeded, for example by a firewall. Ports 3048, 443, and 80 are also required. Technical support will only be provided for the most recent version. Schoellerbank Business Banking supports the MBS standard.

As a cross-sector software solution, the Multi Bank Standard Service (MBS Service) makes it possible to access multiple accounts at different banks using a single program.

2. Digital signature

Transactions can also signed using a qualified digital signature (e.g. the citizen’s card function on an e-card or a.sign premium).

For verification purposes, the information about the orders to be completed is also displayed. In the case of transfer orders, the payee’s IBAN and the transfer amount or a reference code and control value (total amount of all orders) are included. The Customer is required to check that this information matches the submitted orders. The signature PIN may only be entered if the information is correct.

This signature method is not an application of the Bank. If it is necessary to block or cancel the certificate, this must be handled through the certificate provider.

3. Use through other software products (MBS Service)

Customers can also use MBS through the software products of other banks (e.g. Business Line or ELBA Business) that permit a connection to be established with Schoellerbank’s data processing centre. Depending on how these software products manage user permissions, the user and any parties who have been given read-only authorisation may be able to access data and information pertaining to the registered accounts. The hotline of the bank that provided the main licence for MBS is responsible for responding to Customer queries regarding this application.

PC282E - 023GI9210E 20200101

Annex to the terms and conditions of electronic banking

Recommendation from the Bank to ensure security on the Internet and when using Electronic Banking

1. The Electronic Banking system relies on the Internet, which is an open and publicly accessible communication medium. An unauthorised third party could use a Customer's personal identifiers to gain access to the Internet banking system and complete transactions using the (securities) account of the Customer. The Bank provides regular information on its website www.schoellerbank.at and directly in Internet banking about current dangers on the Internet and also provides concrete recommendations and security notices as to how to minimise the risks arising from these dangers when using Internet banking. For this reason, Customers are strongly advised to exercise particular caution when conducting transactions via Internet banking to avoid damages.

2. The Bank takes considerable measures to secure the data transmitted via Electronic Banking and processed by the Bank and has comprehensive security precautions in place to protect against attacks during data transmission over the Internet and during data processing on the Bank servers. To ensure that these security precautions are not circumvented, the Bank advises every Customer to employ technical measures of their own to protect the systems and computers that they use. The Bank provides information about potential dangers on its website and in Internet banking and the required and recommended security measures for protecting the Customer's systems and computer.

PC282E - 023GI9210E 20200101