Expobank

Terms and Conditions for the Use of Internet Banking Services

Expobank CZ a.s.

Contents:

1. Subject Matter and Applicability

1.1 In accordance with the General Business Conditions ("**GBC**") and the Terms and Conditions for the Payment System ("**Payment Terms and Conditions**"), Expobank CZ hereby issues the Terms and Conditions for the Use of Internet Banking Services ("**Special Terms and Conditions**") to lay down rights and duties relating to the use of the Internet Banking system.

1.2 The Special Terms and Conditions complement the Payment Terms and Conditions and the GBC, and constitute a part of specific agreements between the Client and the Bank as regards the grant of access to direct banking, wherever such a specific agreement contains a reference to that effect.

1.3 In the event there is a discrepancy between the provisions of a specific agreement and the provisions of these Special Terms and Conditions, the Payment Terms and Conditions, and the GBC, the provisions of such a specific agreement take precedence. Any matter not defined under a specific agreement is subject to these Special Terms and Conditions, the Payment Terms and Conditions, and the GBC in the foregoing order.

2. Definitions

Where written starting with a capital letter, the following terms used in these Special Terms and Conditions have the meaning defined below or, as the case may be, in the GBC:

Access Rights – A set of authorizations defining the accounts and other services to be used and administered via Internet Banking and persons authorized to use such accounts and other services, including the definition of the scope and manner of the foregoing rights.
Administrator – An Authorized User to whom the Client grants a power of attorney under an application for establishment or change of access to Internet Banking services empowering the Authorized User to order products and services offered through Internet Banking.
Agreement – Agreement for the use of Internet Banking services entered into between the Bank and the Client, or another agreement defining the Client's access to Internet Banking based on such an agreement.
Authenticator – A technical device for eCode access that, after one of its functions is selected, generates and displays an Authorization Code for access to Internet Banking or a Signature Code for the entry of an Order.
Authorization Code (OTP) – A string of characters generated for the Client by an Authenticator as a confidential identifier verifying the Client's identity.
Authorized User – A natural person who has been granted Access Rights to the Client's account(s) and other products used by the Client through Internet or Mobile Banking based on the Client's request to the extent determined by the Client.
Bank – Expobank CZ a.s. with registered office at Na strži 2097/63, 140 00, Prague 4, Identification No. 14893649, registered under Reg. No. B 476 in the Commercial Register maintained by the Prague Municipal Court.
Bank Data – Data in electronic form intended for transmission, where the exchange of such data constitutes the subject of provided services.
Bank's Website – The website at http://www.expobank.cz/.
Biometric data – Personal data of technical nature allowing the unique identification of the Client using physical and physiological characteristics of a natural person.
Client – The holder of an account maintained by the Bank who signs the applicable Agreement and determines Authorized Users for Internet Banking.
Client Center – The Bank's client service and contact center that provides access to the Bank's selected services through remote communication means. The Client Center can be accessed using the contact details posted on the Bank's Website.
Daily limit for payment transactions – Maximum daily limit for CZK payments made from the Client's account(s).
eCode Access – Access to Internet Banking allowing the use of both Information and Payment Services.
ePIN Code – Personal identification number (if the Bank made it available to the cardholder) provided solely to the cardholder and used exclusively for the authorization of 3D Secure payment transactions carried out using a payment card.
GBC – The Bank's General Business Conditions.
Information Services and Configuration – Services provided by the Bank through Internet Banking specified in Article 4.1 of these Special Terms and Conditions.
Internet Banking – For the purposes of these Special Terms and Conditions, Internet Banking means the Bank's Internet Banking system available at https://expobanking.cz/.
Mobile Application – An application used to control accounts maintained by the Bank, logging in, authorization of payment orders and requests submitted via Internet banking through mobile devices.
Mobile Banking – Internet banking controlled via a Mobile Application.

Notification – Requested SMS or e-mail messages through which the Bank informs the Client of matters related to the use of services.
Order – An order or request submitted by the Client to the Bank through Internet Banking as part of Payment Services.
Password – A string of letters and/or other characters allowing SMS access and GA code access to Internet Banking.
Payment Services – Services provided by the Bank through Internet Banking specified in Article 4.2 of these Special Terms and Conditions.
PIN – The Client's personal identification number used to verify the identity of the person entering the code.
Security Code – A code sent to the Client as part of SMS access by the Bank via an SMS message to confirm a change of the Password during the first login to Internet Banking and during every subsequent change of the Password or for signing a payment order or a report sent to the Bank by the Client through Internet Banking.
Signature Code (SIGN) – A string of characters generated for the Client by an Authenticator as a measure for securing a transaction as well as for identifying the Client during the entry of an Order as part of Payment Services.
SMS Access – Access to Internet Banking allowing the use of both Information and Payment Services; SMS Access may only be established for mobile numbers offered by Czech and foreign Mobile operators.
Special Terms and Conditions – The Bank's business terms for the use of Internet Banking services, which complement the GBC and the Payment Terms and Conditions.
Third Party – An entity licensed and authorized to provide services consisting of the indirect placement of a payment order and/or the provision of account information.
User – A natural person, the Client or an Authorized User for Internet Banking, with defined Access Rights for the Client's accounts and products.
User Name – The name under which the Client logs into Internet Banking.

3. Requirements for the Use of Internet and Mobile Banking

3.1 Technical requirements for Internet and Mobil Banking:
A description of the technical requirements for the use of Internet and Mobile Banking is available on the Expobank CZ website at www.expobank.cz. The Client must review and comply with the technical requirements.

3.1.1 Hardware – The Client's device used for Internet Banking must meet the minimum configuration requirements of the provider of the applicable web browser.

3.1.2 Software – The current version of the following web browsers is required – Windows Internet Explorer, Mozilla Firefox, Safari, or Google Chrome.

3.1.3 To access Mobile Banking, the Client must have the Mobile Application installed on his/her mobile device. The Mobile Application can be downloaded from the provider of applications based on the operating system used by the Client's mobile device. The Mobile Application is distributed by the Bank using official channels through Google Play and App Store. The Client must refrain from installing the Mobile Application from sources other than the foregoing official sources.

3.2 By signing the Agreement, the Client guarantees compliance with the Bank's technical requirements for the use of Internet and Mobile Banking services. The Client acknowledges that a failure to use the required software and/or hardware prevents the Bank from guaranteeing the flawless use of Internet and Mobile Banking.

3.3 The Bank reserves the right to change the technical requirements for Internet and Mobile Banking to ensure that the Client will be able to use Internet and Mobile Banking to its full potential following any improvement or expansion of services.

4. Overview of Main Services Provided through Internet and Mobile Banking

4.1 Information Services and Configuration provided through Internet Banking:

(a) Overview of the Client's accounts
(b) Display of detailed information on the Client's accounts
(c) Current balance of the Client's accounts
(d) Statements of transaction history on the Client's accounts
(e) Statements of the Client's accounts in the PDF format
(f) Messages – a service allowing the bidirectional sending of text messages; attachments can be enclosed with messages

(g) Change of the Password for login into Internet Banking
(h) Notification configuration – SMS or e-mail messages used by the Bank to inform the Client of transactions relating to the Client's products
(i) Overview of investment products
(j) Overview of credit products
(k) Overview and maintenance of Third Parties
(l) Additional services to selected Accounts

4.2 Payment Services

(a) Domestic payment orders – the Bank accepts payment orders submitted by the Client internally within the Bank and outside the Bank within the Czech Republic, where the account and transaction currency may be the Czech crown or other currencies
(b) Foreign payment orders – the Bank accepts payment orders internally within the Bank, orders for payments abroad, and payments within the Czech Republic in Czech crowns and in other currencies
(c) Payments between the Client's own accounts in the currency of one of the accounts without the need for payment authorization
(d) SEPA payment orders – the Bank accepts SEPA payment orders in EUR internally within the Bank and to EU/EEA countries
(e) Direct debit authorization/SIPO in favor of an account in the Czech Republic
(f) Configuration of domestic and foreign recurring payment orders

4.3 Card Services

(a) Display of payment card transactions
(b) Display of information on limits and change of card limits
(c) Activation of payment card-related insurance
(d) Blocking of a payment card
(e) Configuration of PIN code for payment card
(f) Configuration of telephone number and ePIN code for payment card for the 3D Secure service
(g) Application for the issue of a new payment card

4.4 Delivery of Documents

The Bank and the Client agree that documents (agreements, annexes to agreements etc.) relating to products and services may be delivered by the Bank through the electronic repository (document archive) in the Internet Banking application. The Bank and the Client further agree that the Client is entitled to deliver documentation (mainly applications) relating to product and services to the Bank through the Internet Banking. The Bank and the Client also agree that the Bank is entitled to unilaterally reject documents delivered by the Client through the Internet Banking while the Bank may do so without providing reasons. In case the Bank rejects documents provided by the Client through the Internet Banking, the Bank must notify the Client thereof. The Bank and the Client agree that documents delivered by the Client through the Internet Banking will be in PDF format.

4.5 Mutual Communication

The Bank and the Client agree that mutual communication between the Bank and the Client may have the form of messages sent through Internet Banking.

4.6 Applications for Products and Entry into Agreements

The Bank and the Client agree that agreements, annexes to agreements and other related documentation pertaining to products and services offered by the Bank may be entered into through Internet Banking, whereby the Client's handwritten signature is substituted by an electronic signature consisting of the transmission of an Authorization Code to the Bank through an act performed by the Client through Internet Banking. Such form of legal act will be permitted only in cases determined by the Bank.

4.7 Mobile Banking

Mobile banking enables logging in, authorization of payment orders and requests submitted via Internet banking and control of accounts maintained by the Bank to the extent allowed by the Mobile Banking application.

5. Access to Internet and Mobile Banking

5.1 The Bank only provides Internet and Mobile Banking services if the Client has an account or uses a product allowing the use of Internet or Mobile Banking by the Client and by Authorized Users designated by the Client, provided that the Client enters into the applicable agreement with the Bank, where the Bank provides access to Internet Banking to Authorized Users only to the extent of Access Rights defined by the Client.

5.2 An agreement between the Client and the Bank may be entered into in person at one of the Bank's branches, through Internet Banking, or through online registration on the Expobank Website. If the Bank is in possession of the Client's valid specimen signature for the account for which Access Rights are to be established, the Bank may enter into an agreement with the Client even if the Client does not sign the agreement before a Bank officer, on condition that the Client's signature on the agreement unmistakably identifies the person who signed the agreement.

5.3 An integral part of the Agreement is an Application for the Establishment or Changes of Access to Internet Banking Services ("**Application**"). The Client must submit a duly filled out and signed Application to the Bank at one of the Bank's branches, send it with officially certified signature to the Bank or, if the Bank enables the Client to do so, send it through the Internet Banking. Based on the Application, the Bank will establish specific Access Rights for accounts and designated products to the designated extent, including Access Rights for Authorized Users. An Application also serves as a basis for changing existing Access Rights or establishing new Access Rights. The Client may establish and change Access Rights for Authorized Users through Internet Banking.

5.4. The Account Holder may establish, change, or revoke Access Rights granted to Authorized Users through Internet Banking or in person at one of the Bank's branches. The Account Holder may empower another Authorized User under a power of attorney to carry out the administration of Authorized Users through Internet Banking. Likewise, Access Rights granted to an Authorized User may be revoked at any time by means of the Client's written instruction sent to the Bank by fax at the fax number designated for this purpose. If such an instruction is delivered to the Bank during office hours, the Authorized User's access will be blocked without undue delay; if it is delivered outside office hours, access will be blocked on the working day following delivery.

5.5 The Client and Authorized Users may use Internet and Mobile Banking 24 (twenty-four) hours a day. The Bank may reduce or suspend the operation of Internet and Mobile Banking for the duration of necessary maintenance.

5.6 Unless otherwise specified in the Agreement, the Bank only establishes SMS Access for the Client and for Authorized Users.

SMS Access:

5.7 In using SMS Access, the User logs into Internet Banking using the User Name, Password and Security Code send via SMS message.

5.8 The Bank sends the User a SMS message containing a one-time Password to the telephone number designated by the User. The one-time Password can be used only for the first login into Internet Banking, after which the User must change the Password. The first and any subsequent Password change must be confirmed by the User by entering a Security Code provided to the User in an SMS message sent to the User's designated mobile telephone number after such a change is made. A Password selected by the User remains valid until its next change, which may be made solely by the User. The Bank recommends changing the Password at least once a month.

5.9 For the purposes of authorizing a payment order or a request, the User will receive a Security Code from the Bank by SMS message, the entry of which will serve as a signature confirming the relevant payment order or request.

5.10.1 The Security Code is sent to the Users at their risk. The Bank is not liable for a failure to deliver the Security Code or for the delivery of an invalid code as a result of circumstances outside the Bank's control, including, without limitation, error or interruption in telecommunication or a technical defect in transmission devices.

5.10.2 Each User is entitled to use the Mobile Application for logging in, authorization of a payment order, or authorization of a request submitted via Internet Banking as an alternative to a Security Code. The User can

use both authorization methods simultaneously.

eCode Access:

5.11 If the Client applies to the Bank for the establishment of eCode Access, the Bank will, following the entry into the applicable agreement and the delivery of a duly filled out and signed application for the establishment of access to Internet Banking, issue to the Client, or an Authorized User empowered by the Client, a User Name for eCode access and provide the Client or the Authorized User with an Authenticator at the applicable Bank branch.

5.12 The User must choose their PIN upon the receipt of the Authenticator.

5.13 The User logs in to Internet Banking by entering the User Name and an Authorization Code generated by the Authenticator following the entry of the PIN.

5.14 The User must protect the Authenticator from loss and third-party misuse. The Client can apply in writing for the issue of a new Authenticator in the event of loss or damage. Every issue of an Authenticator is subject to a fee as per the Bank's current List of Fees.

5.15 If the User uses an Authenticator requiring an Authorization Card for eCode access, the conditions for the use of standard payment cards apply to the use of a payment card that functions an Authorization Card.

5.16 The Client is entitled to request from the Bank a change of access to the Internet Banking from current SMS access to eCode access and conversely or alternatively request the issue of new Authenticator. The Client shall request the issuance of new Authenticator at a Bank branch or through application with officially certified signature while the officially certified signature is not required if the Client signs the application in front of an employee of the Bank. The Bank gives the Authenticator to the User or sends it to the User's address just as the Authenticator PIN code. In case the application for the change of access to the Internet Banking from current eCode access to the SMS access is accepted, further steps are specified in Article 5.8 of these Special Terms and Conditions.

Access to Mobile Banking:

5.17 The User logs into Mobile Banking by entering the PIN Code or Biometric Data. Verification via Internet Banking is required for the activation of access to Mobile Banking.

5.18 The User must protect the device on which the mobile application is installed from loss and third-party misuse. On mobile devices (particularly smartphones and tablets) using the iOS, Android, Windows Phone, or another operating system, which are used for access to Internet or Mobile Banking or which contain a SIM card containing a telephone number designated for receiving SMS text messages from the Bank, the User must refrain from installing applications from sources other than official sources for the applicable operating system used by the mobile device, such as App Store, Google Play, Window Phone Store, etc.). Furthermore, the Bank informs the Users that they may not rely on checks carried out by the provider of the operation system in relation to all applications.

6. Receipt of Orders for Payment Services

6.1 The Bank processes submitted Orders only until the end-of-day closing time. Closing times are announced by the Bank and are available to the Client at the Bank's branches, at the Client Center, and on the Bank's Website.

6.2 If the Bank receives an Order on a day that coincides with the requested due date after the closing time for the applicable transaction type, the Bank may process the transaction on the following Bank Business Day.

6.3 As part of Information Services, the Bank provides the Client with information allowing the identification of transactions, the transaction sum and currency, and, where applicable, the Order currency and the applicable exchange rate.

6.4 The Bank is only liable for received and confirmed data, and assumes no liability for direct and indirect damage incurred as a result of any erroneous or repeated transmission of data to the Bank, for damage caused by defects in an employed telecommunication network or the Internet, and for technical defects on the Client's side, and damage caused by an act of God (as per Section 2913 paragraph 2 of the Civil Code). Furthermore, the Bank assumes no liability for delays in the execution of foreign payment orders, if delay is caused by the Bank's requests for documents made in accordance with laws and regulations in effect (such

as documents demonstrating the purpose of a payment and documents certifying compliance with information duties laid down in foreign-currency regulations). If the Client fails to provide the Bank with documents necessary for making a payment, the Bank is under no obligation to make such a payment.

6.5 The Bank may set a maximum daily limit for transfers of funds made through Internet Banking. The Limit is specified in the relevant Application. The limit may be set based on an agreement with the Client or unilaterally by the Bank. SMS access to the Internet Banking system involves increased risk of misuse and the incurrence of damage. If the Client requests a limit higher than proposed by the Bank for this type of access, the Client acknowledges and accepts such increased risk. The Bank may change the limit unilaterally in consideration of legal restrictions and the Bank's security policy. Where applicable, the Client will be informed of a change in the limit in a suitable manner sufficiently in advance.

6.6 Other matters relating to the execution of the Client's payment Orders are subject to the Payment System Act and the applicable provisions of the Payment Terms and Conditions and the GBC.

7. Irregularities, Internet and Mobile Banking System Defects, Servicing

7.1 The Client and Authorized Users must inform the Bank immediately of any defect in Internet or Mobile Banking and provide a description of such a defect.

7.2 If the Client or an Authorized User enters the wrong User Name, Access Password or a Security code for SMS Access three times consecutively or enters the wrong User Name, PIN code, or Authorization Code for eCode Access three times consecutively on the Internet Banking login page, the Client's access to Internet Banking will blocked automatically for 15 minutes. The Client can contact the Bank's Client Center, where the operator will restore access to Internet Banking after identifying the Client.

7.3 The Bank may block the access of the Client and an Authorized User to Internet and Mobile Banking if it suspects that the security of the Client's account(s) is compromised. In such a case, the Bank must inform the Client that access has been blocked and of the reasons without unnecessary delay. The Client's and the Authorized User's access to Internet and Mobile Banking will be restored only when the danger of misuse has expired or when appropriate measures have been taken. The Client or an Authorized User may request the Bank to block access to Internet Banking or to Mobile Banking. Blocking access to Internet Banking or Mobile Banking suspends the provision of Third Party services.

7.4 The Bank reserves the right to unilaterally change the Client and Authorized User’s type of access to Internet Banking to an access type providing a higher degree of security. Where applicable, such a change is free of charge.

8. Client Liability

8.1 The Client and, where applicable, an Authorized User, must protect their login data, i.e. the User Name and Password for SMS Access, SIM card used for the Password and Security code delivery, Authenticator, PIN code for eCode, PIN code for login to Mobile Application, Security code and login information to e-mail address used for the Internet Banking, against loss or misuse, to keep login data confidential, to refrain from disclosing login data to any third party. The Client must inform the Bank immediately of the loss of login data or suspicion that login data have been misused through the Customer Service Center at 844 844 822 or +420 233 233 233 (Mon-Fri 8:00 a.m. – 7:00 p.m.); the contacts are available at www.expobank.cz. In addition, the Client must ensure that Authorized Users protect their login data in the same manner. The Bank will be held liable for no damage incurred by the Client as a result of login data loss or misuse if the Bank does not receive information to that effect from the Client.

8.2 The Client acknowledges that the OTP Code in the case of eCode Access and the Password and Security Code in the case of SMS Access and the PIN Code or Biometric Data for the Mobile Application serve to verify the identity of the Client or the identity of an Authorized User, for the purposes of access to Internet Banking.

8.3 Transactions and tasks authorized by a Signature Code (SIGN) and an Security Code and the PIN Code or Biometric Data for the Mobile Application are considered transactions completed by the Client. The Client is fully liable for any and all transactions completed to the debit of the Client's account through remote access, which are duly verified by means of the entry of an Authorization Code or a Security Code.

8.4 The Client must refrain from disclosing any facts pertaining to technical and organizational security measures and measures preventing the misuse of access to Internet and Mobile Banking. The Client must inform the Bank immediately if the Client's or an Authorized Person's login data, the Password or the PIN code in particular, are disclosed or if the Client suspects that the Client's access to Internet and Mobile

Banking has been misused. In addition, the Client must ensure that all Authorized Users conform to these requirements.

8.5 The Bank will block access to the Client's accounts through Internet Banking if the account is misused or if the Client reports loss or disclosure of login data or suspects that misuse of access may have taken place. The Bank will inform the Client without undue delay that the Client's access has been blocked. The Client's access to Internet Banking will be restored only when the danger of misuse no longer exists.

8.6 The Client must immediately verify transactions executed by the Bank as to their conformity to Orders submitted by the Client or by an Authorized User. The Client must inform the Bank in writing of ascertained discrepancies immediately, no later than five (5) Bank Business Days after ascertaining the same. If the Client fails to do so, the Client will bear partial responsibility for any damage thereby incurred.

8.7 The Bank bears no liability for damage incurred as a result of a violation of the applicable Agreement, the Special Terms and Conditions, the Payment Terms and Conditions, or the GBC by the Client or an Authorized User, or as a result of a failure to comply with instructions given by the Bank to the Client or to an Authorized User.

8.8 If a third-party application is used in connection with the use of Internet Banking, the Bank is not liable for the use of such an application or for information received via such an application.

9. Claims

Claims and complaints regarding the operation of Internet Banking and erroneously executed Orders are processed and settled in accordance with the rules and by the deadlines laid down in the Bank's Complaint Rules, which are published on the Bank's Website.

10. Termination of the Business Arrangement

10.1 The business arrangement between the Bank and the Client may be terminated unilaterally by the Bank or by the Client at their discretion, unless otherwise mutually agreed. The ways of termination of the business relationship, the duration of a notice period and other information about the termination of a contract are governed by the GBC, unless otherwise stipulated in the relevant individual contract, Payment Terms and Conditions or these Special Terms and Conditions.

10.2 The Agreement will terminate upon the closing of the Client's account for which Access Rights have been established. If Access Rights have been established for multiple accounts, the Agreement will expire upon the closing of the last of such accounts.

10.3 Both a Client and the Bank may terminate the Agreement in a written form. If a Client submits a termination notice, the Agreement shall terminate upon expiry of the notice period, which is one month from the date of delivery of the notice to the Bank. If the Bank submits a termination notice, the Agreement shall terminate upon expiry of the notice period, which is two months from the date of delivery of the notice to the Client.

10.4 A Client and the Bank may agree in writing to terminate the Agreement on the agreed date.

10.5 The Bank may terminate the Agreement in writing with immediate effect if the Client commits a violation or repeated violations of the provisions of the applicable Agreement, the Special Terms and Conditions, the Payment Terms and Conditions, the GBC, or security instructions given by the Bank to the Client with regard to the use of Internet Banking by the Client, as well as in the other cases laid down in the GBC.

11. Miscellaneous

11.1 The Bank may amend these Special Term and Conditions unilaterally in accordance with Article 44 of the GBC. Amendments to these Special Terms and Conditions made in response to technology-related changes relating to access to and the functioning of the Internet Banking system and the necessity to ensure the continuity of the provision of Internet Banking services in relation to the Client, or made in response to a change in the scope of services provided in the framework of Internet Banking are considered amendments of routine and administrative nature within the meaning of Article 44.5 of the GBC, and, as such, do not require the service of a prior notice to the Client in order to enter into effect. Moreover, the Bank reserves the right to change unilaterally the telephone number of the Client Center and the opening hours during which the Client Center is available to Clients.

11.2 The Bank will inform the Client of any and all changes concerning the Special Terms and Conditions

and the functioning of the Client Center in an appropriate manner, for instance by means of a message sent through the Messages service provided in the framework of Internet Banking, through the Bank's Website, by stating information on an account statement, etc.

These Business Terms and Conditions governing the Use of Internet Banking are valid and effective from November 20, 2020 (the "**Announcement Date**") in relation to new Clients. In relation to existing Clients of the Bank who entered into a contractual relationship with the Bank before the Announcement date, these Business Terms and Conditions governing the Use of Internet Banking shall take effect on February 8, 2021 and replace the existing Business Terms and Conditions governing the use of Internet Banking Services.