Rules for Safe Use of Electronic Banking

The purpose of this document is to provide you with information pursuant to Act No. 492/2009 Coll. on Payment Services before concluding a framework agreement and in particular an agreement enabling the use of electronic Banking services.

The provider of the electronic Banking services is UniCredit Bank Czech Republic and Slovakia, a.s., with its registered office at Želetavská 1525/1, 140 92 Prague 4 – Michle, registered in the Companies Register of the Municipal Court in Prague, Section B, File No. 3608, ID No. 64948242, in relation to the pursuing of banking activities in the territory of the Slovak Republic by means of UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky, Šancová 1/A, 813 33 Bratislava, ID No.: 47 251 336, registered in the Companies Register of the Bratislava III Municipal Court, Section: Po, File No.: 2310/B; The Bank provides its services in the Slovak Republic on the basis of a single banking licence according to the European Union laws, namely based on Notification No. 2013/5785/570 of the Czech National Bank as of 20 May 2013 and Notification No. OBD-5659/2013 of the National Bank of Slovakia as of 4 July 2013 on the conditions for operation of the foreign bank branch in the territory of the Slovak Republic based on a single banking licence (the "Bank").

The Bank provides you as a Client/User with electronic banking services enabling you, via the Internet, to operate agreed banking products such as an account, payment card, loan, bank guarantee, insurance, investment, etc., to negotiate them, to conclude the relevant product contract and also to ensure secure communication between you and the Bank.

1. Personal security features used for user authentication ("Security Features")

The features used for your authentication are unique security features that allow you to access electronic Banking and use our services. We have either assigned these features to you or you have chosen them yourself. Each feature is of a certain type:

a) Knowledge – i.e., something that only the user knows
b) Ownership – i.e., something that only the user has
c) Inherence/Biometrics – something the user is (unique user information)

If at least 2 features are used for authentication, each of which must be from a different category, this is called "strong user authentication".

Personal security features are as follows:

Feature	Description
PIN code for the mobile app	The numeric code for the EB Mobile App, which is used for activation, login or transaction confirmation.
Password for login	The password consists of numeric characters (length 6 characters). It is used to log in to EB Web applications in combination with a one-time text message code. The user is obliged to change the initial password provided by the Bank immediately.
Security key (Smart key, Business key)	A feature included in the EB Mobile Applications for logging into the EB Applications or for authorising payment transactions and other requests, or for generating one-time codes for logging into or authorising transactions in the EB Web Applications even without the device being connected to the internet, i.e. offline.
Hardware security key (token)	A PIN-protected hardware device that is used to generate one-time numeric codes for logging in or authorising transactions in EB Web Applications.
Text message key	Combination of a password and one-time codes sent via text message to the User's mobile phone for logging in or authorising transactions on EB Web Applications.
Registered mobile phone number	Telephone number that the User communicates to the Bank and that allows to receive one-time security codes, called OTP text message (OTP stands for One-Time Password, i.e. a one-time password).
Registered e-mail address	The e-mail address that the user provides to the Bank and that allows the user to receive one-time security codes (OTP e-mail).
Fingerprint (biometrics)	A fingerprint stored on the mobile device on which the EB mobile app is activated.
Face scan (Face ID - biometrics)	A facial scan stored on a mobile device where the EB mobile app is activated. The facial scan is compared with biometric data stored in the Bank or with a photograph (e.g., from an identification document).
Password	A password consisting of various alphanumeric characters used to authenticate the User in different situations.
One-time security password (OTP = One-Time Password)	A one-time security password that can be used to verify the ownership of a security feature. It is a code sent to a registered mobile phone number, to a registered email address or generated by the EB mobile app.
Username	An assigned or, in certain cases, separately configurable name (alias) for logging into the EB Application.
User number	Number assigned to the User by the Bank.
Identity card	User's document issued by a public administration authority, which shows the user's name, surname, date of birth and facial features (ID card, driving licence, passport).
Birth number	User's birth number.

UniCredit Bank

Control question	A question about the User or their products.
CVV2/CVC2	Code A special three-digit number that is shown on the payment card. It is a security feature used to identify the cardholder in a card-not-present environment (e.g., the Internet).
Payment card number	Unique 16-digit payment card number
Electronic signature	Indication of specific data that replace the User's handwritten or even authenticated signature in the computer

2. Rules for the safe use of electronic banking

a) Do not use passwords and PINs in other applications and on the Internet (e.g., e-shops, social networks, emails, etc.) that are identical to the passwords and PINs used for logging in to EB or for authorising payment transactions,
b) set your password and PIN so that it cannot be easily guessed or deduced, e.g., by combining upper and lower case letters, numbers, special characters, etc.,
c) do not disclose to others or enter your personal security feature anywhere on the internet unless it is an electronic banking application on the site https://sk.unicreditbanking.eu, https://sk.unicreditbanking.net/ or https://corporateportal.unicreditgroup.eu/container/sk/login,
d) do not write down passwords and PINs, protect them from disclosure and change them immediately if they have been disclosed or if you have any suspicion that such a situation may have occurred,
e) take extra care when entering personal security features in public (e.g., on public transport vehicles) or in monitored areas (e.g., near security cameras) so that they cannot be seen by others,
f) do not log in to electronic banking unless you are sure that no malicious program can be installed on the device or unless you are in complete control of the device (e.g., in public internet cafés, on computers used by several people),
g) communicate the password for communication with the Bank only to a Bank employee in a situation where this password is required,
h) protect the unlocking and use of the SIM card on your mobile device with a PIN code and, if lost or stolen, have the SIM card blocked immediately by your operator,
i) protect your profile with your mobile operator and do not allow a third party to issue a new SIM/eSIM for your phone number,
j) do not allow others to access your email account and set up two-factor authentication,
k) do not allow another person to access your mobile device (e.g., fingerprint, face scan, password, PIN code),
l) if your mobile device or SIM card is lost or stolen, notify the Bank immediately and have electronic banking blocked as a precautionary measure,
m) do not allow another person's (or family member's) biometric data to be registered on the mobile device,
n) secure access to your mobile device with a password, PIN code or biometric (fingerprint, face scan) and do not leave your mobile device unattended or without the device automatically locking the screen after a short period of time,
o) do not use software modifications to your mobile device that allow full administrator access (e.g., jailbreak, root),
p) regularly update the operating system of your mobile device and individual installed applications,
q) use the latest version of security software on your mobile device (e.g., antivirus, firewall),
r) do not allow unnecessary permissions in newly installed or updated apps on your mobile device (e.g., access to text messages, easy setup, etc.),
s) only install apps from the official app stores – Google Play (for Android), App Store (for iOS) – including any add-ons; if the app you are using asks you to install them, set your mobile device to prohibit the installation of apps from unknown sources,
t) do not install apps based on instructions or requests from a third party, and do not allow a third party to remotely access your mobile device (e.g., via the Any Desk app),
u) unless necessary, do not log on to the computer as an administrator, but as a normal user,
v) update your operating system and programs regularly, especially your web browser; install browser extensions (plug-ins) only on a limited basis and only from well-known and trusted publishers,
w) use the latest version of security software (e.g., antivirus, firewall) and update it regularly,
x) protect your computer from unauthorised access by setting access permissions, password security or other features; do not allow a third party to access your computer remotely (e.g., via Any Desk applications),
y) enter the Bank's website address manually; to access the EB web application site, enter www.unicreditbank.sk, from there go to the internet banking login page, make sure you are accessing the web address https://sk.unicreditbanking.eu, https:// sk.unicreditbanking.net/ or https://corporateportal.unicreditgroup.eu/container/sk/login and do not use a proxy for the internet banking login page,
z) do not access the e-banking services via a link from a search engine or a link sent by email, text message or any other means (on a social network, via a chat application, etc.),
aa) do not log in if the electronic banking login screen looks suspicious to you,
ab) contact the Bank immediately if you register a transaction that you did not authorise,
ac) do not respond to phone calls that invite you to take action with your account, as the Bank never invites its customers to make any transactions over the phone,
ad) do not open an e-mail containing the Bank's name unless it comes from the domain: unicreditbank.sk or unicreditgroup.sk; do not open attachments of a non-standard file type (e.g., extensions: .exe, .php), and do not click on links contained in an untrustworthy message,
ae) familiarise yourself with the messages sent by the Bank to the electronic banking services, especially if they are fraud warnings.

3. Other rules to follow to increase the likelihood of not losing your funds

a) Check what you are confirming
   (i) Before confirming your login or authorising a payment transaction, always check that the details entered (e.g., amount, beneficiary) match your intention.
   (ii) If someone wants to send you money, there is no need to confirm their action. Do not click on links sent to you, and never enter your security features into any app at the request of another person.

b) Monitor the activity on your account
   (i) Knowing what payments have been made on your accounts is the best early warning tool that something is wrong. Therefore, have SMS messages, e-mails or notifications sent automatically to your mobile phone (called push notifications) with information about your transactions.
   (ii) If there is a higher risk activity on the account (e.g., activation of Mobile Banking, change of contact details, etc.), we will inform you by an appropriate message (e.g., push notification, e-mail, SMS).
   (iii) If you register an operation that you did not perform, please contact us immediately on the Bank Infoline.

c) Never respond to phone calls encouraging you to take action with your account
   (i) It is probably a fake banker, a fake policeman or a fake employee of a state institution (National Bank of Slovakia, National Security Authority, etc.). the Bank never invites its clients to make any transactions over the phone, whether it is a withdrawal from an account, a payment transaction or even a loan application.

d) Keep up to date with news about internet safety
   (i) The more information you have, the safer you can be online. So keep up to date with the latest internet safety news and follow all the recommended guidelines.

e) Read the messages sent to you
   (i) E-mails, letters and other messages are not always fun. They are often important and worth reading carefully. This also applies to messages sent to your mobile phone.

f) Contact Bank Infoline
   (i) Respond to any safety alerts you may receive if a risk event occurs. In the event of a suspected fraud or security threat, Bank shall inform the client in an appropriate manner, using the primary contact details provided by the client when concluding the agreement.

4. Authorisation (signature) of an active operation/payment transaction and cancelling a payment transaction

Bank allows clients/users to sign various types of active operations – e.g., a payment order, an agreement, a document or other action. The authorisation method varies from one app to another and is as follows:

In the EB Mobile Applications, authorization takes place in one of the following ways, when the User is asked to do so:
a) by fingerprint or by putting (scanning) the face to the device,
b) by entering a PIN code.

In the EB Web Applications, login and authorisation is performed in one of the following ways:
a) Security Key, namely:
   (i) Smart key - Online method - the User receives a push notification in the EB Mobile App and after opening the app, signs the transaction with a fingerprint, face scan or by entering a PIN code.
   (ii) Smart Key - Offline Method - EB Web App displays a QR code which the User scans via the Smart Key in the Smart Banking Mobile App, which generates a 6-digit one-time code. The User enters this code in the login section of the Online Banking Web Application and confirms it.
   (iii) Business Key - Offline method for logging into BusinessNet Professional, BusinessNet and Trade Finance Gate - User generates a 6-digit code to log in with the Smart Key in the Business Smart Banking or BusinessNet Mobile app.

b) Text message key
   This method consists of a combination of a personal password and one-time codes sent to the User's mobile phone. The User enters his/her password on the EB Web Application screen and the Bank sends a text message containing a one-time code to the designated mobile phone. This time-limited code is typed by the User back into the EB Web Application to confirm the operation.

c) Hardware security key (token)
   The password to sign the operation is generated by the token. The User enters the PIN code on the token keypad. If the correct PIN code is entered, the token generates an 8-digit one-time code, which the User enters into the Web application. The app then displays a 6-digit one-time code, which the User types back into the app to authorise the transaction.

A payment transaction is cancelled in the same way as its authorisation, if the cancellation is enabled by the respective app.

UniCredit Bank

5. Liability for loss of funds in the event of loss, theft, misuse or unauthorised use of a means of payment or personal security feature

a) Please report immediately any unauthorised or incorrectly executed payment transaction, loss, theft, misuse or unauthorised use of your means of payment or personal security feature, personal documents, mobile phone with a stored payment card, activated Mobile Banking or anything suspicious in connection with Internet or Mobile Banking to the line +421 2 6828 5777 (24/7, non-stop) or at any of our branches during opening hours. In such a situation, Bank will block the account to which any of the above security incidents are related.

b) You are liable for the loss of funds resulting from an unauthorised payment transaction up to an amount equivalent to EUR 50 if the loss was caused by the use of a lost or stolen means of payment or personal security feature or by the misuse of a means of payment or personal security feature as a result of your negligence, except as set out below.

c) You do not bear any financial loss if:
   (i) it arises from the use of a lost, stolen or misused means of payment from the time you report this fact to the Bank; however, this does not apply if you have acted fraudulently; or
   (ii) the loss, theft or misuse of the means of payment could not have been detected by you prior to the payment transaction; this does not apply if you have acted fraudulently.

d) You will bear all losses related to unauthorised payment transactions if they are caused by your fraudulent conduct, your wilful failure to comply with one or more of your obligations to provide personal security features, or your failure to comply with one or more of these obligations as a result of your gross negligence.

6. Liability for a defectively executed payment transaction

It is a defectively executed payment transaction if Bank has not settled the amount of the payment transaction in the correct currency or has not used the account number or other unique identifier in accordance with your order.

If Bank is obliged to correct a defectively executed payment transaction and you notify Bank that you do not insist on executing the payment transaction, Bank will immediately...

a) restore your account to the state it would have been in if this debit had not occurred, or
b) refund the amount to your account, as well as the transfer fee and interest lost if the procedure under a) is not applicable.

If you do not notify Bank that you do not insist on executing the payment transaction, Bank will immediately...
c) ensure that the amount of the incorrectly executed payment transaction is credited to the beneficiary provider's account, and
d) restore your account to the state it would have been in if Bank had executed the payment transaction correctly, or
e) refund to you the incorrectly paid fee and the lost interest if the procedure under (a) is not applicable.