Rules for Safe Use of Internet Banking

Valid from 2 September 2024

The purpose of this document is to provide you with information pursuant to Articles 133 and 134 to 139 of Act No. 370/2017 Coll. on Payment System before concluding a framework agreement and in particular an agreement enabling the use of Internet Banking services.

The provider of the Internet 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 (hereinafter referred to as the "UniCredit Bank"), tel. +420 221 210 031, e-mail: info@unicreditgroup.cz. UniCredit Bank's activities are supervised by the Czech National Bank with its registered office in Prague, delivery address Na Příkopě 28, 115 03 Prague.

As a client/user, you can use certain banking services, communicate with UniCredit Bank in an agreed manner and, in particular, authorise the relevant payment transactions or other orders as part of the Internet Banking in the Smart Banking or Online Banking app via the Internet. Any confirmation, consent or other action of a similar nature made by you in the Internet Banking when using the relevant personal security feature shall be deemed to be a binding expression of your will.

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 Internet Banking and use Smart Banking or Online Banking app products, including authentication of the user's identity through Bank iD. We have either assigned these features to you or you have chosen them yourself. Each feature is of a certain type:

a) Knowledge (K) – i.e., something that only the user knows
b) Ownership (O) – i.e., something that only the user has
c) Inherence/Biometrics (I) – 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 client authentication".

Personal security features are:

Feature	Description	Type
PIN for mobile app	A numeric code for the SmartBanking mobile app that is used to activate, log in or confirm transactions. This PIN is non-transferable, is set by the user and **can only be known by the user** (similar to a payment card PIN). This PIN is only used in the SmartBanking app.	K
Password	The password consists of numeric characters (length 6 characters). It is used to log in to Online Banking (in combination with a one-time SMS code). The password is non-transferable and can only be known by the user. The user must immediately change the initial password to their own. The password is used only in the Online Banking app (at cz.unicreditbanking.eu).	K
Activated mobile app (SW security key)	The Smart Banking mobile app contains a "security key" (Smart Key). Once activated, the app is uniquely associated with the user. The app allows the user to receive push notifications, which can be used to confirm login to Online Banking or authorise a payment transaction. The app allows the user to generate one-time codes for logging in or signing transactions in Online Banking offline (without connecting your mobile device to the internet).	O
Hardware security key (HW token)	A hardware device that generates a PIN-protected code. It is used to generate one-time numeric codes for logging in or authorising payment orders.	O
Registered mobile telephone number	A telephone number assigned to the user at UniCredit Bank that allows the user to receive one-time security codes, called SMS OTP (OTP stands for One-Time Password).	O
Registered e-mail address	An e-mail address assigned to the user at UniCredit Bank. The e-mail address allows the user to receive one-time security codes (OTP e-mail).	O
Fingerprint (biometrics)	A fingerprint stored on the mobile device on which the SmartBanking mobile app is activated. It is used for login confirmation or transaction authorisation in the activated mobile app (SW security key).	I
Face scan (biometrics)	A face scan stored on the mobile device on which the SmartBanking mobile app is activated. It is used for login confirmation or transaction authorisation in the activated mobile app (SW security key). The face scan is compared with biometric data stored by us or against your photograph (e.g., from an identification document). It is used, for example, for strong client authentication when activating a mobile app (SW security key).	I

Password for communication with the bank	A password consisting of various alphanumeric characters (length 6-14 characters). This password is used to authenticate the user when contacting UniCredit Bank by phone.	K
One-time security password (OTP = One-Time Password)	A one-time security code that can be used to verify ownership of the security feature. It is a code sent to a registered mobile telephone number, registered e-mail address or generated by the SmartBanking mobile app. **Never forward or disclose** this security code **to third parties**. This code is used when activating Mobile Banking, logging into Internet Banking (when using the SMS OTP method), verifying a new telephone number, resetting your PIN, etc.	O

Other features used for authentication:

Feature	Description
Username	Username (assigned number or chosen alias) used to log in to Internet Banking
Personal documents	User's personal documents (ID card, driving licence, passport).
Birth certificate number	The birth certificate number assigned to the user.
Control questions	Questions about the client or their products.
CVV2/CVC2 code	A special three-digit number that appears on the payment card. It is a security feature used to identify the card holder in an environment without the presence of a payment card (e.g., the internet)
Payment card number	Unique 16-digit payment card number

2. Rules for features: PIN/Password

a) Don't use the same passwords and PINs as in other applications and on the internet (e.g., online shops, social networks, e-mails, etc.). Set your security feature (password, PIN) so that it is not easily guessable or inferable (e.g., based on your date of birth, username). Use strong passwords – the longer and more complex the password, the higher the security (e.g., combination of upper and lower case letters, numbers, special characters, etc.)

b) Do not disclose your security features to anyone or enter them anywhere on the internet, unless it is UniCredit Bank Online Banking and Smart Banking. Enter your Mobile Banking PIN only in the SmartBanking app (during activation, login and transaction confirmation). Enter your password (Online Banking) only in Internet Banking at https://cz.unicreditbanking.eu. Never enter your mobile app PIN into the website or share it with anyone. This PIN is never required by an employee of the Police of the Czech Republic, the Czech National Bank or UniCredit Bank. The PIN for your mobile app is one of the most important security features you need to protect.

c) Do not keep passwords and PINs in an easily readable form (e.g., by writing them down on paper, in an unencrypted file on your computer) and protect them from disclosure.

d) In the event that your password or PIN has been compromised, or you merely suspect that it has been compromised, change your password or PIN immediately.

e) Take extra care when entering security features in public (e.g., on public transport vehicles) or in monitored rooms (e.g., near security cameras). Make sure that the information you enter cannot be seen by others.

f) Don't enter your security features on computers (e.g., when logging into banking) where you can't be sure there are no malicious programs installed (e.g., public internet cafés, computers shared by multiple people).

g) The password for communication with the bank should only be given to a UniCredit Bank employee in a situation where this password is required. Fill in this password or part of it only in the selected passworded documents sent by the Bank. The password for communication with the bank should only be given to a UniCredit Bank employee in a situation where this password is required.

3. Rules for features: activated mobile app, hardware security key, registered mobile telephone number, registered e-mail address, one-time security password

a) These features must be protected from unauthorised access by third parties. Use your PIN to unblock and use your SIM card. If your mobile device is lost or stolen, a third party will not be able to receive your security codes (OTP). Even so, have the SIM card blocked by your operator as soon as possible.

b) Protect your profile with your mobile operator. Never allow a third party to have a new SIM/eSIM issued for your telephone number.

c) Do not allow others to access your e-mail account and set up two-factor/two-step authentication).

d) Do not allow others to access your mobile device (e.g., fingerprint, face scan, password, PIN) or install malicious software on your mobile device.

e) If your mobile phone (or SIM card) is lost or stolen and a third party can access your SMS messages and make calls from your telephone number, contact UniCredit Bank immediately and have your Internet Banking blocked as a precaution.

4. Rules for features: fingerprint/face scan

a) The SmartBanking app can use biometric data (fingerprint, face scan) stored on your mobile device. Only you decide whether to allow the use of biometric data for user authentication when you activate or in the SmartBanking app settings. Never allow another person's (or family member's) biometric data to be registered on your mobile device.

5. Rules for mobile devices used to access the Smart Banking app

a) Secure access to your mobile device with a password, PIN or biometrics (fingerprint, face scan). Don't leave your mobile device unattended and use the automatic device (screen) lock after a short period of time.
b) Do not use software modifications to your mobile device that allow full administrator access (e.g., jailbreak, root).
c) Regularly update the operating system of your mobile device and individual installed apps.
d) Use the latest version of security software (e.g., antivirus, firewall) on your mobile device and update it regularly.
e) Do not allow unnecessary permissions (e.g., SMS access, facilitation, settings, etc.) in a newly installed or updated app on your mobile device. A malicious app with broad permissions can track you, including the security features you enter, and send them to a third party (attacker).
f) Only install apps from the official app stores – Google Play (Android), App Store (iOS) – on your mobile devices including any add-ons that the app you are using asks you to install. Set your mobile device to ban the installation of apps from unknown sources.
g) Do not install apps based on someone else's instructions and, in particular, do not allow strangers to access your mobile phone remotely (e.g., via the AnyDesk app).

6. Rules for devices used to access the Online Banking app

a) Don't log into Internet Banking on devices when you can't be sure there are no malicious programs installed (e.g., public internet cafés, computers shared by multiple people). If you have any doubts about the safety of the device, do not use it. Ideally, log in from a device that you have full control over, such as your home computer.
b) Do not log on to the computer as an administrator unless necessary. Log on to your computer as a normal user.
c) Regularly update your operating system and your programs, especially your web browser.
d) Install browser extensions (plug-ins) on a limited basis and only from known and trusted publishers.
e) Use the latest version of security software (e.g., antivirus, firewall) and update it regularly.
f) Protect your computer from unauthorised access by setting access permissions, password security or other features.
g) Do not allow strangers to access your computer remotely (e.g., via AnyDesk).

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

a) Access to Internet Banking
   (i) Enter the UniCredit Bank website address manually. To access the Online Banking app site, use www.unicreditbank.cz to go to the Internet Banking login page. Make sure you are accessing the web address https://cz.unicreditbanking.eu. Do not use a shortcut to the Internet Banking login page.
   (ii) Never access Internet Banking via a link from a search engine or a link sent by e-mail, SMS or other means (social network, chat app, etc.).
   (iii) If the login screen for Internet Banking products looks suspicious to you, do not log in, as attackers can mimic the appearance of the login page very closely and trick you into logging in subtly, e.g., via SMS, e-mail, etc.

b) User identity authentication via BankID
   (i) Be careful on which sites you are going to use your banking identity.
   (ii) Make sure you control what data you provide and to whom within BankID.
   (iii) When using your banking identity, make sure that you actually enter your security features on the UniCredit Bank website (https://cz.unicreditbanking.eu).
   (iv) Follow the same rules as for Internet or Mobile Banking.

c) 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.

d) 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 at the UniCredit Bank Infoline.

e) 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 (Czech National Bank, National Cyber and Information Security Agency, etc.). UniCredit 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.

UniCredit Bank

f) Handle suspicious messages with caution
   (i) For each e-mail and SMS message, check the address of the actual sender and any web link that the e-mail/SMS prompts you to click on.
   (ii) Messages in various chat apps (WhatsApp, Messenger, etc.) containing an active link may also pose a risk. E-mails from us can only come from the domain: unicreditbank.cz or unicreditgroup.cz. If an e-mail from UniCredit Bank arrives from another domain, do not open it.
   (iii) UniCredit Bank never sends e-mails or other messages asking you to disclose security features. Never respond to such messages and inform us via the UniCredit Bank Infoline.
   (iv) If the message from UniCredit Bank seems suspicious in any way and you are not sure, please contact us via our Infoline. If you have already opened the message, be sure not to open attachments of a non-standard file type (e.g., file extensions: .exe, .php). or click on links contained in the message. If you accidentally do this, close everything quickly and don't let the program or browser install anything. Run a virus scan and let us know.
   (v) Use junk mail (spam, phishing) protection in your e-mail inbox.

g) 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.

h) 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.

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

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

UniCredit 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:

Authorisation in the Smart Banking app

a) Biometric signature – signature by fingerprint or face scan
In this case, the user is prompted to use a fingerprint or face scan.
b) Signature by entering a PIN – signing the operation by entering a PIN. In this case, the user is prompted to use a PIN.

Authorisation in the Online Banking app

a) Smart Key
   (i) Online method – you will receive a push notification to your Smart Banking app on your mobile phone. After opening the message, you check the details of the operation for signature and sign it biometrically or by entering a PIN.
   (ii) Offline method – the Online Banking app displays a QR code, which you scan with the Smart Banking app (its "Smart Key" section), which generates a 6-digit one-time code, which you enter into the Online Banking app and confirm.

b) SMS Key
This method consists of a combination of a personal password and one-time codes sent to your mobile phone.
The user enters their static password. If the correct password is entered, UniCredit Bank will send an SMS message to the user's mobile phone containing a OTP. The user enters this time-limited code back into Online Banking to confirm the operation.

c) Hardware Token
The password for signing an operation is generated by a token (called "calculator"). Access to the security key is protected by a PIN code chosen by the user. The user enters the PIN directly on the token keypad.
If the correct PIN is entered, the token generates an 8-digit one-time code that the user enters in the Online Banking app. The app then displays a 6-digit one-time code (OTP), which the user enters again in the Online Banking app. If the OTP is correct, the operation is successfully signed.

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

9. 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, but no later than within 10 working days, 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, Mobile Banking activated or anything suspicious in connection with internet or Mobile Banking to the UniCredit Bank Infoline: +420 221 210 031 (24/7, non-stop) or at any of our branches during opening hours. In such a situation, UniCredit 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, provided that the following conditions are met at the same time:
   (i) The execution of a payment transaction not authorised by you occurred after you reported the loss, theft, misuse or unauthorised use of a means of payment or personal security feature to UniCredit Bank; and
   (ii) You have not intentionally or grossly negligently breached your duty to protect personal security features.

c) You are fully liable for any loss of funds resulting from an unauthorised payment transaction if you caused the loss by your fraudulent conduct or by your wilful or grossly negligent failure to protect personal security features. Intentional violation of the obligation to protect personal security features or violation of the obligation to protect personal security features as a result of gross negligence shall be deemed to be a failure to comply with the rules set out in this document as well as in generally binding legal regulations.

10. Liability for an incorrectly executed payment transaction

It is an incorrectly executed payment transaction if UniCredit 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 UniCredit Bank is obliged to correct an incorrectly executed payment transaction and you notify UniCredit Bank that you do not insist on executing the payment transaction, UniCredit 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 UniCredit Bank that you do not insist on executing the payment transaction, UniCredit 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 UniCredit 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.