Raiffeisen BANK
Client inspired banking

PRODUCT CONDITIONS FOR DIRECT BANKING SERVICES

(hereinafter also referred to as the „Product Conditions")

1. Availability of Direct Banking Services

1.1. Direct Banking Services are provided on the basis of the Service Agreement concluded between the Client and the Bank. The Service Agreement may also be part of arrangements for other services provided by the Bank to the Client. Obligations under the Service Agreement cannot be terminated or cancelled separately during the term when the Bank provides other Banking Services to the Client. This arrangement stipulates interdependence of services provided by the Bank, as referred to in certain Agreements concluded between the Bank and the Client. If the Bank no longer provides Banking Services to the Client other than Direct Banking Services, obligations under the Service Agreement including obligations under supplementary services pursuant to Article 5 of these Product Conditions shall expire. However, obligations stipulated under Article 4 of the Product Conditions shall survive for the term when the User is allowed to use the Electronic Identification Tool. The Client may continue using the Direct Banking Services even after expiration of the obligations under the Service Agreement for access to information and documents delivered by means of the Direct Banking Services. However, if following expiration of the obligations under the Service Agreement the User does not sign into a Direct Banking Service for 6 months, the Bank is entitled to block the instruments and data used by such User to access the Direct Banking Services. If obligations under the Service Agreement can be terminated, the Bank may do so subject to a 2-month notice, unless the termination notice stipulates a longer period, and the Client may do so subject to a 14-day notice. During the term of obligations under the Service Agreement the Client is entitled to ask the Bank for the contents of the Service Agreement and information that the Bank is obliged to provide to the Client before concluding the Service Agreement.

1.2. In the event that another User accesses Direct Banking Services on behalf of the Client, the Client shall define the scope of the User's authorizations by means of a Signature Specimen. The Signature Specimen may be explicitly identified in another manner, for example as a record on set up access rights. In addition to concluding the Service Agreement, availability of certain Direct Banking Services requires further cooperation between the Bank and the Client or User. The Client, or another person based on authorization granted in a Signature Specimen or by a power of attorney bearing the Client's certified signature or the Client's signature made before an employee of the Bank, is entitled to establish, modify or cancel a Signature Specimen.

1.3. The Bank shall allow selected Clients to specify the initial scope of User authorizations, modify the existing scope of User authorizations or cancel a User role (i.e. to establish, modify or cancel a Signature Specimen) via Direct Banking Services (particularly Internet and Mobile Banking). The administration of user authorizations carried out in this manner will be allowed primarily in respect of Clients who are legal entities and who can be expected to require the establishment of a higher number of Users and more frequent modifications of their authorizations. The above functionality shall only be available to Users accordingly and explicitly entitled by the Client by means of a Signature Specimen (however, such entitlement cannot be granted via Internet Banking). However, Clients who are natural persons will be allowed by the Bank to administer User authorizations according to these provisions even if they do not explicitly establish such authorization as Users. Creation or modification of a Signature Specimen via Internet Banking may only apply to a User who has been properly identified by the Bank within the meaning of Article 2 of GBC.

1.4. When arranging for Direct Banking Services, a Client Number for signing in to the Direct Banking Services shall be assigned to the Client by the Bank or chosen by the Client.

1.5. The Client specifies what Electronic Key the User shall use. Depending on the chosen Electronic Key, the Bank shall provide assistance as required to acquire and use it. In addition, assistance of the User or also the Client is required.

1.6. Use of Internet Banking is conditioned by User's access to a computer connected to the internet. Also, the User must be the holder of a Mobile Device activated in the network of any Mobile Operator.

1.7. Activation and use of Mobile Banking requires the User to meet the prerequisites for access to Internet Banking and to have a Mobile Device with the iOS or Android operating system and an internet connection.

1.8. To use Phone Banking, the User must be the holder of a Mobile Device activated in the network of any Mobile Operator.

1.9. To use the service identified as Premium API, the User must be authorized to acquire the relevant Premium API certificate via Internet Banking and must have access to the required third-party instruments (particularly software) adapted for data communications with the Bank via the Premium API interface.

2. Scope of Direct Banking Services

2.1. Direct Banking Services are a set of Internet, Phone and Mobile Banking, primarily used as a means of communication of the Bank and the Client in respect of the Bank's existing or future services provided to the Client and conditions applicable to the provision of such services including conclusion of contracts, services provided by third parties cooperating with the Bank, as well as the point of delivery of messages or legal acts of the Bank or third parties cooperating with the Bank, addressed to the Client, and as a means of communication for delivery of the Client's Instructions or Instructions on the Agreement to the Bank. The scope of Internet, Phone and Mobile Banking available to the Client also depends on other services provided by the Bank to the Client. In the case of a User who is not a Client the scope of Direct Banking Services available to the User is specified by the Client by means of a Signature Specimen.

2.2. The Bank continuously develops and modifies the services and features available through Direct Banking Services. Also in order to increase the security of mutual communications, the Bank develops and adopts necessary measures that may affect the availability of Direct Banking Services or the Client's access to Direct Banking Services or the method of use of Direct Banking Services by the Client. If required with regard to the nature of newly included services, removed services or modified features of services, the Bank shall inform the Client about the adopted measures in an Appropriate Manner.

2.3. The Client is aware that Direct Banking Services may be used as a means of remote communication for the purpose of concluding Agreements. Agreements requiring written form shall bear an Electronic Signature of the acting contracting party. For the purpose of this

provision of the Product Conditions, an Agreement may also mean a draft Agreement or acceptance of a draft Agreement. An Agreement concluded through Direct Banking Services in written form shall be kept on file by the Bank and its wording shall be provided to the Client at request; also, a concluded Agreement is usually available to the User via Internet Banking. The Client and the Bank agreed that a draft Agreement or its acceptance can be delivered by the Bank to the Client also by means of Direct Banking Services. In such a case, Internet or Mobile Banking is the Client's mailing address for this purpose; the Bank may send the relevant response to the Client (such as rejection or acceptance of a draft) via a different Direct Banking Service than used by the Client to contact the Bank (for example, acceptance of a draft Agreement filed by the Client via Mobile Banking may be delivered to the Client via Internet Banking), or via an entirely different means of communication. The provisions of this paragraph 2.3 shall apply by analogy to any conclusion of services between the Client and third parties represented by the Bank.

2.4. Direct Banking Services may also be used as a means of remote communication for the purpose of delivery of selected documents in electronic form from the User to the Bank. An overview of documents that may be delivered to the Bank in this manner shall be made available by the Bank to the User in an Appropriate Manner, in particular via a dedicated part of Internet or Mobile Banking, along with information about the supported document formats, maximum size of the documents or any further technical or other conditions that must be complied with in order to successfully deliver the document to the Bank. The Bank may also enter into a special agreement with the Client on the conditions applicable to the delivery of a particular document in electronic form. The Bank is not obliged to accept any document not listed in the overview of documents accepted by the Bank or any document that is not subject to a special delivery agreement between the Bank and Client, or any document not delivered to the Bank in accordance with the agreed or available conditions. Availability of this functionality for a particular Client or User may depend on the Bank's sales offer and on the scope of other agreed Banking Services.

2.5. Authentication or Certification Codes or RB Key may be used in connection with the provision of services by the Bank to the Client also in selected situations (such as cash withdrawal) for acts between the Client and the Bank at a Business Location as a supporting means of verification of the User's identity or to confirm a User's Instruction.

2.6. If the User is authorized to acquire and acquires a Premium API certificate, he or she is obliged to treat the Premium API certificate the same way as any other Electronic Identification Tool. Premium API certificates are linked to particular Users and are not transferrable. Access to the Premium API certificate is protected by a password chosen by the User. It then allows the User to submit requests to the Bank only as authorized under the relevant Signature Specimen. The Premium API Certificate allows the User to submit a request to the Bank solely using software that has been adapted by the software maker to communicate with the Bank via Premium API. Thus, the Bank does not guarantee that the User will be able to use the Premium API certificate and bears no responsibility for the software to ensure flawless communications and data transfers via Premium API. The Client is obliged to check that the software to be used by the User to submit requests to the Bank, where the User's identity will be verified using the Premium API certificate, is suitable adapted to such data communications and provides the Client and User with an adequate level of security and protection of the data to be delivered by the Bank via this form of communications at request of the User. Also, the Bank bears no responsibility for the security and confidentiality of data delivered from the Premium API interface. The scope of requests that the User may submit to the Bank via the Premium API interface is limited to the current sales offer of the Bank.

3. Conditions for the Operation of Direct Banking Services

3.1. The Bank operates Direct Banking Services 24 hours a day. Although the technical means required for the use of Direct Banking Services are usually always available to the User, the Bank is under no obligation to allow their use on an uninterrupted and continuous basis. The Bank is entitled to suspend or restrict the provision of Direct Banking Services as necessary for the maintenance of equipment required for their operation.

3.2. The Client is obliged to advise the User of the conditions of Direct Banking Services.

3.3. The Bank is not obliged to check the accuracy of data entered by the User through Direct Banking Services.

3.4. By entering the appropriate Certification Code, PIN or password or another Electronic Identification Tool or a combination thereof, the User expresses consent to realization of the relevant act (particularly Instruction or Instruction on the Agreement) requiring the Certification Code, PIN, password or the other Electronic Identification Tool or a combination thereof. The User may express consent to the realization of selected Instructions (such as orders for outgoing payments between Accounts held by the Bank for the same Client) or Instructions on the Agreement by confirming them in the form of clicking or tapping the corresponding button displayed in the Direct Banking Service or RB klíč (RB Key). Also, the User may express his or her consent to the realization of an Instruction or Instruction on the Agreement by successfully verifying his or her identity using a fingerprint or other biometric data using the biometric data sensor of his or her Mobile Device. The method of expressing the User's consent to the realization of the particular act depends on the technical solution chosen by the Bank that is available to the User when expressing such consent.

3.5. The Bank shall inform the Client in an Appropriate Manner about all relevant facts related to the operation and availability of Direct Banking Services.

3.6. Referring to the update of the Technical Conditions, Article 1.8.4. Maximum Expense Limits, Payment Transactions, for which a Payment Order is placed via Direct Banking Services, are subject to the following limitations:
The biometric data sensor of a Mobile Device can be used to express consent to the realization of a Payment Transaction amounting up to 5,000 CZK. In the case of a Payment Transaction in another currency, foreign exchange rates announced by the Bank in the Exchange Rates List apply to the conversion. However, the Bank is also entitled to request that consent to the realization of a Payment Transaction below 5,000 CZK be expressed otherwise than by using the Mobile Device's biometric data sensor.
As agreed in the Technical Conditions, upon reasonably concluding on the existence of risk of damage on the Client's part, the Bank is entitled to unilaterally change the above limits (particularly to lower them down to 0) and to inform the Client about the adopted measures in an Appropriate Manner.

3.7. The Inform Me service covers the sending of various messages as requested by the User. Messages on Payment Transactions and card holds are only sent if the Payment Transaction amount exceeds a limit set by the User. Also, messages are not sent when the fee for sending the message cannot be charged (such as due to insufficient funds in the relevant Account).

3.8. Operation of Internet Banking
The Bank allows Internet Banking Users to communicate with the Bank through the internet public data network. The address to sign into Internet Banking is posted on the Public Website and may vary depending on the Electronic Key type used by the User.

3.9. Operation of Mobile Banking
The Bank allows Mobile Banking Users to communicate with the Bank through a Mobile Device application using an internet data connection. The application is available for download via the appropriate distribution services according to the operating system or mobile device manufacturer, under the name of "Raiffeisenbank CZ – Mobilní eKonto" or a name that will replace it and about which the Bank will inform the Client in an Appropriate Manner.

3.10. Operation of Phone Banking
The Bank allows Phone Banking Users to communicate with the Bank through the public telephone network. Phone Banking can be accessed via the infoline posted on the Public Website. When calling from abroad, Phone Banking can be accessed also on the infoline posted on the Public Website.

4. Security of Direct Banking Services

4.1. General security principles:

a) A User can have only one Client Number. At request of the User or in the event of suspected abuse of the Client Number, the Bank is entitled to change the Client Number; the Bank shall inform the User about the change immediately. Users shall primarily choose a Client Number that is not directly associated with their identity;

b) Users can only hold one Electronic Key of each type. An exception to this rule is the Smartphone Electronic Key that is unique for every mobile device, used by the User to access the Mobile Banking service; Users can have up to five (5) Smartphone Electronic Keys;

c) Electronic Identification Tools are non-transferable and must not be disclosed in any manner to a person who is not the authorized holder;

d) Electronic Identification Tools are issued solely to be used in connection with services provided by the Bank or services provided or arranged for with the Bank's participation;

e) For security reasons, the Bank is entitled to block any Electronic Identification Tool, particularly in the case of suspected loss, theft, abuse, unauthorized use or fraudulent use of the Electronic Identification Tool, such as if detecting actual or impending use of the Electronic Identification Tool by a person other than the authorized User, if being notified by the User of such abuse, or if being demonstrably informed that the User has died or has been declared dead;

f) The User is obliged to change PINs on a regular basis (at least once every three (3) months) for maximum security of realized Instructions and Instructions on the Agreement. Also, the User is obliged to change the PINs if invited to do so by the Bank;

g) The User is further obliged to not record his or her passwords and PINs in an easily recognizable form and is obliged to not disclose such to this parties. Also, the User is obliged to protect his or her Electronic Identification Tools from theft or abuse by any person;

h) in the event of theft, abuse, loss, unauthorized use or suspected theft, abuse, loss or unauthorized use of Electronic Identification Tools, the User is obliged to immediately report the fact to the Bank in an appropriate manner (particularly by means of the contact details published by the Bank on the Public Website);

i) If the User is approached with a prompt or invitation to enter any Electronic Identification Tools by means of an electronic mail message, mobile text message or another form of electronic communications, the User shall not proceed in accordance with such prompt or invitation and is obliged to contact the Bank, particularly by telephone, using the contact details posted by the Bank on the Public Website and consult any response to such prompt or invitation with the Bank. The User is also obliged to contact the Bank when in doubt as to whether he or she communicates with the Bank or representative of the Bank and if the Bank asks the User so in connection with any activity in respect of which the User is uncertain as to whether it is the intentional and wanted outcome of his or her earlier activities;

j) The User is obliged to proceed with care when online, in particular the User is obliged to:
1) not use publicly accessible technical devices or technical devices, the safe use of which for accessing Direct Banking Services has not been or could not have been verified by the User, to access Direct Banking Services;
2) refrain from visiting websites that are untrusted and may impose a risk for secure use of the Direct Banking Services (particularly websites with any illegal content);
3) pay attention to received e-mail and mobile text messages or other forms of remote communications, not open unsolicited communications and, if the User already does so for reasons of necessary verification of the nature of the message, not open or run any suspicious attachments of such messages or links contained in the messages;
4) always verify whether the website on which the User enters the Electronic Identification Tools is operated by the Bank, particularly according to the content of the address line in the browser that corresponds to „https://www.rb.cz" and according to the security certificate by viewing its detail after clicking the lock icon on the address line in the internet browser („view/show certificate"). The certificate holder (entity) must be Raiffeisenbank a.s. (a detailed description is available in Secure Banking). The secure method of accessing the Public Website chosen by the User for the purpose of signing into Internet Banking shall be manual typing of the above address in the relevant address line of the browser;
5) not enter any Electronic Identification Tools in places other than in the relevant Mobile Banking application, RB klíč (RB Key) application or other communication means agreed with the Bank, or on websites operated by the Bank, and to not respond to requests to enter any Electronic Identification Tools contained in any electronic message;
6) not allow any person to remotely operate the Technical Device when the User uses or accesses the Internet Banking or Mobile Banking service;
7) pay careful attention to the description of the Instruction or Instruction on the Agreement to which a sent Certification Code or requested confirmation in the Mobile Banking or RB klíč (RB Key) application relates. Where it does not conform to the User's desired and intended plans, the User is obliged to not use such Certification Code or to not make such certification;
8) use two different Technical Devices when using Mobile Banking and Internet Banking simultaneously;

k) If the Client uses a Mobile Device to access the Direct Banking Services, he or she is obliged to prevent other persons from using the Mobile Device and applications used to access the Direct Banking Services. Also, the Client is obliged to not allow another person to register any security tools in the Mobile Device that may be used for access to the Direct Banking Services or to express consent to an Instruction or Instruction on the Agreement (such as numeric or

other codes, biometric data), not disclose the data and tools used to access the Direct Banking Services or to express consent to an Instruction or Instruction on the Agreement to another person, and to protect the same against being detected by other persons, and to immediately notify the Bank of loss, theft, damage or abuse or suspected abuse of the Mobile Device or the SIM card contained therein;

l) The Bank shall provide the Client with its current recommendations relating to security of Direct Banking Services and threats that the User of Direct Banking Services may be exposed to, all in a message delivered via Direct Banking Services or another contact (such as in an e-mail or mobile text message, notification in a Mobile Device application), or particularly via Secure Banking. The Client is obliged to always read such instructions, check the contents of Secure Banking on a regular basis, and when using Direct Banking Services to respect and follow the Bank's instructions while taking into account the Bank's information regarding current threats. Also, the Client is obliged to inform each and every User about the contents of such instructions of the Bank and to ensure that each and every User follows such recommendations of the Bank;

m) Use of a Mobile Device's biometric data sensor may be temporarily prevented particularly due to its repeated unsuccessful use; to sign into Electronic Banking Services or to express consent to the realization of an Instruction or Instruction on the Agreement, the User must then use the appropriate PIN, for example;

n) The User is obliged to ensure regular updates of the Technical Device's operating system, equip the Technical Device with functioning and updated antivirus software, including regular antivirus scans of the Technical Device, and to protect the Technical Device using a communication management tool (firewall). Further, the User is obliged to keep track of recommendations and warnings of manufacturers or distributors of software or the Technical Device regarding threats and risks, and adjust the use of the Technical Device or software accordingly;

o) The User is obliged to not install in the Technical Device any software not originating from trusted sources (in the case of Mobile Devices, from relevant official sources according to the Mobile Device's operating system) or any software in respect of which the User is not certain as to whether it is free of any viruses or other similar harmful content that would impose a threat to the User and secure use of the Direct Banking Services. In the case of software installed on the Mobile Device, the User shall pay attention to the authorizations required by the software; when in reasonable doubt that the required authorization is not a threat to secure use of the Direct Banking Service, the User shall refuse to grant such authorizations. The above obligations of the User also apply if the User only uses the Mobile Device for MEk SMS;

p) To access Direct Banking Services, the User is not entitled to use a Mobile Device that has been subject to actions identified as "root/jailbreak" or other interference in order to gain privileged access to the Mobile Device's settings and to overcome limitations set by the manufacturer.

4.2. Electronic keys

Access to Direct Banking Services is protected by Electronic Keys that stand for a security tool for communications between the Bank and Client. An SMS Mobile Electronic Key allows the User to receive unique Authentication and Certification Codes using his or her Mobile Device in the form of SMS text messages. Its use requires the User to declare his or her identity using the Client Number, properly type or tell the Authentication or Certification Code generated by the Bank, and usually also at attach the relevant PIN. A Personal Electronic Key ensures that unique Authentication or Certification Codes are generated directly. A Smartphone Electronic Key is created via a link to the Mobile Device registered in Internet Banking for access to Mobile Banking when activating the service. An RB Key is activated via Internet Banking, or by means of other cooperation of the Bank and User, in a registered Mobile Device and then allows the User to access Direct Banking Services and express consent to the realization of an Instruction or Instruction on the Agreement, usually in combination with the chosen PIN, password or successful use of the Mobile Device's biometric data sensor. If the User is to be provided with an additional or emergency Electronic Key, which requires cooperation with Bank, the Bank shall activate such an Electronic Key within two Banking Days from delivery of such request (activation may be subject to further cooperation of the User or Client).

5. Supplementary Services

5.1. Via its Direct Banking Services, the Bank allows for ordering other services extending the existing Banking Services, such as by new methods of delivery of information about the used Banking Services, or representing separate Banking Services.

5.2. Open Banking

a) Internet or Mobile Banking can be used to take out a service informing about the payment account, which is part of functionalities identified as „Open Banking". The service may be taken out for own needs by any User of Internet Banking; in such case, he or she is a Client to the Bank appearing in own name.

b) The service informing about the payment account allows for concentrating information about payment accounts held with other payment service providers in Internet and Mobile Banking. The information also covers data about transactions made on payment accounts. The scope of information available in Internet and Mobile Banking particularly depends on the data made accessible by the payment service provider maintaining the payment account. The Bank has no influence on the fact whether the other payment service provider makes the information about the particular account accessible or not. Internet and Mobile Banking can be used to concentrate information about payment accounts maintained by providers with whom the Bank is able to ensure the acquisition and forwarding of such information. The Bank's sales offer may change in this regard.

c) For an account included by the Client in the account information service, the Bank shall also ensure update of the data including relating transactions without the Client's assistance. However, such updates can only take place subject to a limited frequency. If the Bank carries out data updates in the maximum possible frequency, any further updates during the relevant period (usually one day) require the Client's explicit instruction (primarily via Internet or Mobile Banking). Depending on development of the technical infrastructure, the Bank shall allow the Client to structure and display the linked payment account information in various manners.

d) The data acquired by the Bank for the Client when providing the payment account information service in respect of accounts held with other payment service providers and about the relating payment transactions are solely used to provide the payment account information service, unless the Bank and Client agree otherwise, or unless the Client grants consent to another use of the data.

e) Provision of the payment account information service is subject to existence of the Service Agreement.

5.3. RB Identity

a) RB Identity services can be solely used via RB Key (RB klíč). RB

Identity services are not available for other Electronic Key variants.

b) For the purpose of using RB Key as part of RB Identity, the Bank shall ensure that Users are able to use this Electronic Key as a means of electronic identification or for other purposes as required for the National Point services or in other relationships with third parties that intend to rely on the services ensured by the Bank as part of RB Identity. The scope of such services depends on the Bank's business offer and readiness of third parties or intermediary providers of identification services to use RB Identity services. However, the Bank is obliged to ensure that Users are particularly able to use RB Key as a means of electronic identification for National Point services.

c) Using RB Key within RB Identity services particularly for the needs of National Point services requires that RB Key becomes a means of electronic identification as part of the electronic identification system within the meaning of the legal obligations applicable to the Bank as the administrator of such system. These obligations require the Bank to deliver to the National Point records the information about the RB Key that is available to the particular User along with information about the level of assurance, i.e. indication of the degree of confidence that a third party may have in authentication using RB Key. Further, the Bank is obliged to authenticate the RB Key holder via the National Point.

d) User authentication via the National Point takes place by means of the number and type of the User's document, which may be supplemented, for unambiguous identification, by the name and surname, domicile address, date and place of birth. The type of the User's identity document must be subject to records in the population register. However, identity cannot be verified by means of the National Point if the information about the number and type of the User's document available to the Bank does not match the document held by the User at the time of such verification and the Bank cannot establish the current data concerning the number and type of document without the User's assistance. RB Identity cannot be provided without successfully verifying the User's identity via the National Point.

e) The Bank shall perform the activities pursuant to paragraph 5.3, points c) and d) above on the basis of the provisions contained in these Product Conditions in relation to the Users who are Clients and thus have entered into a Service Agreement with the Bank. Thus, RB Identity services will be available to them already on the basis of the agreement contained in these Product Conditions. However, this does not apply in cases where identification of the Client upon the conclusion of the Banking Services has not taken place in the Client's physical presence with an identity document recorded in the population register or electronically using a recognised electronic identification means issued by another bank or a provider of identification services. As soon as RB Identity services are available to the User, the User shall promptly verify via Direct Banking Services that his or her identification data registered by the Bank are accurate and up to date.

f) The Bank shall make available RB Identity services to Users who are not parties to a Service Agreement or fail to meet the prerequisites according to paragraph 5.3, point e) on the basis of RB Key registration for the needs of RB Identity services, particularly via the Internet Banking. However, successful registration requires compliance with the conditions stipulated in paragraph 5.3, point e), i.e. verification of the User's identity in his or her physical presence by means of an identity document recorded in the population register and consequent successful verification of identity via the National Point. Also, the Bank allows Users to cancel the RB Key registration as a means of electronic identification within RB Identity. The arrangements contained in paragraph 5.3, point f) shall apply to RB Key re-registration of registration of a newly activated RB Key by analogy.

g) Third parties or intermediary providers of identification services may also stipulate other additional conditions for RB Identity Users, such as a minimum age. However, the Bank only provides information concerning the User to third parties only if and to the extent that the User has consented to it. The above does not apply in the case of the Bank's activities pursuant to points c) and d) above towards the National Point; such procedure is already applied by the Bank on the basis of the agreement on RB Identity services contained in paragraph 5.3 of the Product Conditions.

h) Using RB Key for RB Identity purposes is subject to the same security principles as stipulated for Direct Banking Services in Article 4 of the Production Conditions. The User is liable for damages caused by abuse of RB Identity that occurred through breach of these security principles as a result of the User's negligence, all until the moment of reporting pursuant to paragraph 4.1, point h) of the Product Conditions.

6. Liability for Damages

6.1. The Bank is not liable for damages resulting from the reasons and to the extent as agreed in the relevant provisions of GBC, particularly for damages caused by temporary unavailability of Direct Banking Services, telephone network failures, data network failures, or failures on the part of a mobile operator or internet service provider. In the event that Payment Services are provided by means of Direct Banking Services, liability for damages of the Bank and the Client shall be governed by arrangements contained in the Technical Conditions.

7. Out-of-Court Resolution of Disputes

7.1. In the provision of services to which these Product Conditions apply, also the relevant financial arbiter has jurisdiction to resolve disputes between the Bank and the Client who is a Consumer, if Czech courts otherwise have jurisdiction over such disputes. If the Client who is a Consumer does not agree with the Bank's steps in the provision of services to which these Product Conditions apply, he or she may refer his or her complaint to the financial arbiter operating at Legerova 69, 110 00 Prague 1. More information and contact information is available on the financial arbiter's website at www.finarbitr.cz.

8. Final Provisions

8.1. The Bank is entitled to propose an amendment to these Product Conditions under the conditions and in the manner agreed in Article I of GBC.

8.2. These Product Conditions become effective as of 1 September 2021 and supersede the Product Conditions for Direct Banking Services that became effective on 1 June 2021.

9. Terms and Definitions

Capitalized terms not defined in these Product Conditions are defined in GBC.

Authentication Code means a numeric code serving to verify the User's identity in Direct Banking Services. The code can have either limited or unlimited validity; however, it is always a one-time code that cannot be reused.

Secure Banking means a section of the Public Website identified as "Secure Banking", available via links on the "Important Information" tab on the Public Website in its bottom part, or directly at

https://www.rb.cz/bezpecne-bankovnictvi.

Certification Code means a numeric code serving to sign an Instruction or an Instruction on the Agreement, generated using an Electronic Key. The code can have either limited (online Certification Code) or unlimited (offline Certification Code) validity. However, it is always a one-time code that cannot be reused.

Electronic Identification Tools mean all types of tools and data for verification of the User's identity and to express consent to an Instruction or Instruction on the Agreement. These include Certification and Authentication Codes, PINs, passwords, Premium API certificate, as well as RB Key or a Mobile Device (particularly its hardware and software equipment), if the User uses for example his or her biometric data to sign into Direct Banking Services or to express consent to an Instruction or Instruction on the Agreement.

Electronic Keys mean tools allowing the User to verify his or her identity towards the Bank or to approve an Instruction or Instruction on the Agreement. Variants of Electronic Keys available to the User depend on the technical and security solution of mutual communication selected by the Bank, as well as the Bank's sales offer. Electronic Keys are also identified as security tools in contractual documents, particularly in Signature Specimens.

Information Message means a SMS text message sent to the designated telephone number or a text message sent to the User's e-mail address, or a notification of the Mobile Banking application, to inform the User about Account balance or movements or about other facts. Delivery of a notification requires functioning data transfers of the Mobile Device used by the User to access Mobile Banking; the notification will not be delivered if data transfers are unavailable.

Inform Me means a service for sending Information Messages.

Internet Banking means a service (system) operated via a client application run in the web browser environment, communicating with the Bank's server.

Client Number means a unique numeric indication of the User's identity for Direct Banking Services, not serving to verify the User's identity.

SMS Mobile Electronic Key or also SMS MEk allows the User to receive online Authentication and Certification Codes in the form of a regular SMS text message on a Mobile Device. Such delivered codes can be used in Phone Banking if combined with T-PIN or in Internet Banking if combined with I-PIN.

Mobile Banking means a service operated by means of a client application on a Mobile Device and communicating with the Bank's server.

Mobile Operator means an electronic communications service provider.

Mobile Device means a mobile telephone or another mobile device (tablet). Where the use of a Mobile Device requires the use of services of a Mobile Operator, the Mobile Device must be equipped with a SIM card activated in a Mobile Operator network.

National Point means the National identification and authentication point serving for verification of identity of persons when using online public administration services.

Personal Electronic Key or also PEk means a hardware device allowing the User to generate online and offline Authentication and Certification Codes. Its use is protected by a PIN.

PIN means a multi-digit numeric code used by the User to approve an Instruction or Instruction on the Agreement. The PIN is intended for use in Internet, Mobile or Phone Banking and is identified as I-PIN, T-PIN or S-PIN for the purpose of the respective Direct Banking Services. Also, the PIN is one of the security elements to approve an Instruction or Instruction on the Agreement using a Mobile Key or to use PEk. Upon repeated unsuccessful attempts to enter the PIN, the Bank is entitled to block its further use. The number of such unsuccessful attempts varies depending on the particular PIN type. If the PIN is blocked, the User asks the Bank for required assistance to reinstate access to Direct Banking Services.

Premium API means the Bank's interface to provide selected Banking Services to Clients. Users with required authorizations may acquire and maintain a Premium API certificate that allows them to access certain services of the Bank using third-party software equipment (such as via an accounting system). Premium API particularly includes an opportunity to collect the Client's Account transaction history in this manner. If other Premium API functionalities become available in the future to control or use the Bank's services, Clients and Users will be informed accordingly in an Appropriate Manner.

RB Identity means a Banking Service that particularly stands for electronic identification or authentication of the User using RB Key through or in cooperation with the Bank and towards third parties. Also, RB Identity may enable the User to perform legal acts towards third parties, all to the extent as currently offered by the Bank or intermediary providers of identification services.

RB klíč (RB Key) means a stand-alone application or additional feature of Mobile Banking ensuring secure communications between the User and Bank when using Direct Banking Services. The stand-alone application is available for download via the appropriate distribution services according to the operating system or Mobile device manufacturer. RB Key allows the User to verify his or her identity towards the Bank or to express consent to the realization of an Instruction or Instruction on the Agreement. To operate RB Key, it is necessary to enter a PIN (if RB Key is used as a feature of Mobile Banking, it is also the S-PIN) or password or to successfully use the Mobile Device's biometric sensor.

Direct Banking Services mean Internet, Mobile and Phone Banking services.

Smartphone Electronic Key or also SPEk means a functionality in the Mobile Banking application serving to protect communications between the User and the Bank when combined with an S-PIN.

Service Agreement means the agreement between the Bank and the Client to arrange for Direct Banking Services.

Phone Banking means a service allowing the User to communicate with a representative - phone banker - of the Bank in order to get information about services provided by the Bank or to use certain services of the Bank directly.

Technical Device means a Mobile Device, computer or notebook used by the User to access and use Direct Banking Services.

User means the Client or another individual authorized by the Client to access Direct Banking Services and to use other services on behalf of the Client as provided by the Bank via Direct Banking Services, all to an extent defined by the Client. In the case of the payment account information service, the User is a person taking out the service in own name and as such always is a Client.