PPF Banka

BUSINESS CONDITIONS OF PPF banka a.s.
FOR THE USE OF INTERNETBANKING SERVICES

CONTENTS:

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

1. INTRODUCTORY PROVISIONS

1.1. These Business Conditions of PPF banka a.s. for the Use of Internetbanking Services (hereinafter the "Conditions") set out the basic rules applying to business relations between the Bank and its Clients during the use of the Internetbanking Banking Service.

1.2. Capitalised terms or phrases used in these Conditions have the meaning specified in the article "Definition of Terms" in the General Business Conditions of PPF banka a.s. (hereinafter the "GBC") and/or the article "Definition of Terms" herein, or, where applicable, the meaning specified in the individual provisions hereof. Such defined terms and phrases apply both to the singular and the plural similarly.

1.3. These Conditions have been issued under, and in accordance with, Section 273 of the Commercial Code, the Payments Act, the Banking Act and any associated legal regulations.

1.4. These Conditions constitute "Specific Business Conditions" (hereinafter "SBC") issued in accordance and conjunction with the GBC. Any relations between the Bank and the Client not provided for under these Conditions shall be governed by the GBC.

1.5. These Conditions form an integral part of the Agreement on Internetbanking concluded between the Client and the Bank. Should the Agreement on Internetbanking contain provisions at variance with these Conditions, the provisions of the Agreement on Internetbanking shall prevail. Should these Conditions contain provisions at variance with the provisions of the GBC, the provisions of these Conditions shall prevail.

2. DEFINITION OF TERMS

2.1. **Authorisation** – the process during which a User approves a Payment Order or a request made to the Bank by means of a Certificate, an OTP code or an SMS code.

2.2. **Authorisation Right** – a rule providing authorisation to view selected Accounts from the List of Accounts, to submit Payment Orders from particular CAs and to perform their Authorisation, or to send requests to the Bank. The Authorisation Right also specifies the method by which Authorisation is to be performed, and forms an annex to the Agreement on IB.

2.3. **Security Elements** – in accordance with the GBC these consist primarily of the following: a Certificate, a Certification Token, an OTP code, an OTP Token, a PIN for Certification Token, an IB Login Password, an SMS code and an IB Username.

2.4. **CA** – a current account.

2.5. **Certification Centre** – the internet application of the registration authority. The Certification Centre handles the creation and renewal of Certificates.

2.6. **Certification Token** – the USB device on which a Certificate is stored.

2.7. **Certificate** – a personal certificate generated by the Certification Centre which verifies a User's identity. This is not, however, an encrypted signature.

2.8. **Batch** – a file in a specific format (generated e.g. by the Client's accounting system) whose content is a multiple Payment Order.

2.9. **Supplier** – a third party that processes or performs a service or services forming part of IB, or which contractually carries out activities for the Bank associated with the operation of IB.

2.10. **IB (also "Internetbanking")** – an online system of ELB (operating via a continuous connection with the Bank) allowing a User to communicate with the Bank, to submit Payment Orders and requests to the Bank, and to obtain additional information, including information about the balance on Accounts and any Payment Transactions performed on them.

2.11. **Limit** – the maximum total amount that may be used in handling Funds in a CA based on an Authorisation Right. This Limit is always specified in CZK, is associated with a specific Authorisation Right, and may be set for a Payment Order (hereinafter also referred to as the "Transaction Limit"), for a certain time period (day, week or month – hereinafter also referred to as the "Time-based Limit"), or in a combined form for a Payment Order and also for a certain time period. A Limit applies in aggregate to all the CAs which may be handled via IB based on an Authorisation Right.

2.12. **Rights** – the general term used for both Authorisation Rights and Viewing Rights. These Rights are specified in an annex to the Agreement on IB.

2.13. **OTP code** – a unique, six-digit numerical identifier for authorization purposes which a User generates by means of an OTP Token separately for:

- each login to IB, to enable User verification,
- each Payment Order or request sent to the Bank, for the purpose of their Authorisation.

This is not, however, an encrypted signature.

2.14. **OTP Token** – a device or application used to generate an OTP code. This is provided as:

- a hardware device (hereinafter also referred to as a "Hardware OTP Token"), or
- a mobile application (hereinafter also referred to as a "Software OTP Token").

2.15. **PIN (Personal Identification Number)** – the code for access to the Certification Token on which the Certificate is stored. A PIN must have between six and twenty characters, may contain only alphanumeric characters without diacritical marks, must include at least one uppercase letter, one lowercase letter and one digit.

2.16. **Viewing Right** – a rule authorising a User to view selected Accounts from the List of Accounts, and potentially to enter Payment Orders from particular CAs or to send requests to the Bank. A Viewing Right does not authorise the User to perform the Authorisation of Payment orders, even in conjunction with a User holding an Authorisation Right.

2.17. **IB Login Password** – assigned to a User if Authorisation via an OTP code and an SMS code

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

has been chosen. The User enters the IB Login Password when logging into IB and when performing the registration of the OTP Token. An IB Login Password must have between six and ten characters, may contain only alphanumeric characters without diacritical marks, must include at least one uppercase letter, one lowercase letter and one digit, and may not contain any repetitions.

2.18. **List of Accounts –** a list of the Accounts which may be viewed or potentially handled via IB. The List of Accounts forms an annex to the Agreement on IB.

2.19. **Agreement on a CA –** an Agreement on a Current Account concluded between the Bank and a Client.

2.20. **Agreement on IB –** an Agreement on Internetbanking concluded between the Bank and a Client.

2.21. **SMS code –** a unique, eight-digit numerical identifier for authorization purposes which is sent to the User to a specified Czech mobile telephone number. A unique SMS code is generated separately for:

- each login to IB, to enable User verification,
- each Payment Order or request sent to the Bank, for the purpose of their Authorisation.

This is not, however, an encrypted signature.

2.22. **Token –** the general term used for both the Certification Token and the OTP Token.

2.23. **User –** a natural person authorised by a Client in the Rights to actively use IB, i.e. in particular to handle Funds on a CA to which the Client has given the User access rights via IB, to perform the Authorisation of Payment Orders and requests submitted to the Bank, and to send Authorised messages to the Bank. A User is an Authorised Party within the meaning of the GBC.

2.24. **User Guide –** the Bank's set of rules for the use of IB. The Bank may amend the User Guide. The current version of the User Guide is published by the Bank on its Website. The User Guide does not constitute Information within the meaning of the GBC.

2.25. **IB Username –** a User's login name for IB agreed between a Client and the Bank and stated in the User's Rights. An IB Username must have between eight and sixteen characters, may contain only alphanumeric characters without diacritical marks, must include at least one uppercase letter, one lowercase letter and one digit.

2.26. **Multiple Authorisation –** a system configuration where a selected number of Authorisations from (2 or more) Users is required for the use of IB, regardless of the amount of any specified Limit.

2.27. **Multilevel Authorisation –** a system configuration where a selected number of Authorisations from (1 or more) Users is required for the use of IB, depending on the amount of a specified Limit.

2.28. **Customer Service –** a telephone number or email address used for reporting faults or irregularities in IB and for providing user support to Clients and Users. Customer Service is available on Business Days from 8.00 a.m. to 6.00 p.m.

3. GENERAL PROVISIONS

3.1. IB is established upon the conclusion of an Agreement on IB. All legal relations associated with IB are governed by the laws of the Czech Republic.

3.2. Clients and Users are obliged to familiarise themselves with the content of the Agreement on IB, these Conditions, the User Guide, the Security Principles and the GBC, and undertake to adhere to them. The Client shall at all times bear full liability for cases where Users violate the conditions stated in any of the documents above.

3.3. In the List of Accounts, the Client is to specify the basic CA from which Fees for the establishment and administration of IB and for other services associated with IB service provision are to be debited. The preferred currency used for this CA is CZK. It may be denominated in a currency other than CZK only if the Client does not have any CA held in CZK connected to the IB.

3.4. Other Fees associated with Payment Transactions and Payment and Banking Services are debited from the particular Accounts via which the respective Payment Transaction was performed or the respective Payment or Banking Service was provided.

3.5. Clients access IB through the Website. Clients may use IB only for the agreed purpose. Clients use IB via Users.

3.6. The Client acknowledges that, based on the respective Rights, Users have access to information regarding the balance and the transactions performed on the Accounts which they work with.

3.7. The performance of payments via IB is governed by the GBC, unless these Conditions or the Agreement on IB state otherwise.

4. TECHNICAL REQUIREMENTS

4.1. Software (SW):
Desktop version of the Windows operating system supported by the manufacturer.
Web browser – the following are supported by the Bank:

- Mozilla/Firefox in the manufacturer's supported version,
- MS Internet Explorer in the manufacturer's supported version.

A PDF file viewer is required to display CA statements.
In order to log in using a Certificate the following are also required:

- Token SW – an application used for managing the Certification Token; the supported operating systems for this SW are Windows XP and above,
- drivers to ensure the correct functioning of the Certification Token,
- Java Runtime Environment, version 1.5 and above,
- BSC applet for communication with the Certification Token.

In order to log in using an OTP code generated by a Software OTP Token it is also necessary to have a mobile application to generate the OTP code. The supported operating systems for this mobile application are iOS, Android and BlackBerry. The

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

Bank has the right to (permanently or temporarily) restrict the range of operating systems supported.
To submit Payment Orders in the form of Batches we also recommend having SW to generate the Batch file in a format supported by the Bank.

4.2. Hardware (HW): a personal computer connected to the internet. The speed and quality of this internet connection must be sufficient to allow operations to be performed in IB within the set security time limits.

4.3. The Bank may improve IB from time to time by upgrading the system to a higher version; the Bank is obliged to inform Clients of any such planned upgrade sufficiently in advance of performing the upgrade.

4.4. Clients are obliged to ensure that they have HW which is adequate in terms of its functioning and performance and that any other installed SW is compatible with IB for the entire period of validity of the Agreement on IB. In cases where IB is improved and/or upgraded to a higher version, Clients are obliged to ensure that their HW and SW meet the requirements for this change.

4.5. By signing the Agreement on IB the Client guarantees that it has adequate HW and SW for IB use.

5. SERVICE IMPLEMENTATION

5.1. The Bank will conclude an Agreement on IB with the Client only if the Client holds at least one CA with the Bank.

5.2. The Bank will provide the Client with access to use IB following the signing of the Agreement on IB and the submission of the respective annexes to the Agreement on IB duly completed and signed by the Client and the Users.

5.3. When signing the Agreement on IB the Client shall specify a List of Accounts and Users, including their Rights. The Client may change these specifications at any time.

5.4. If the Client closes the CA that is given in the List of Accounts as the basic CA, the Client is obliged to specify a new basic CA in the List of Accounts.

6. SECURITY

6.1. IB is secured against abuse using Security Elements.

6.2. To ensure secure access to IB the Bank primarily uses a public key infrastructure (PKI). This ensures that all security needs are met by means of asymmetric encryption and Certificate-based User authentication as a means for non-repudiation and data integrity. To ensure secure access to IB the Bank may also make use of other Security Elements (e.g. an OTP code, an SMS code etc.), and may collect and evaluate information relating to Users' access to IB. Actions for which Authorisation is given by an authorised User are binding for the Client.

6.3. Each User may log in to IB and perform Authorisation by one method only – either using an OTP code, an SMS code or a Certificate. The method used may be changed based on a request from the Client.
The Bank has the right to (permanently or temporarily) restrict the range of methods available for Authorisation and/or the means used for obtaining them.

6.4. Data is automatically encrypted during transfer between the Client and the Bank.

6.5. After the signing of the Agreement on IB, the following will be provided in accordance with the Agreement and in the agreed manner depending on the chosen means of Authorisation:

- Authorisation using an OTP code:
  - the IB Login Password will be provided only to the User, either in a secure envelope or via an SMS message;
  - if the User will be using a Hardware OTP Token to generate OTP codes, this OTP Token will be handed over in person either to the Client or to a person authorised by the Client;
  - ff the User will be using a Software OTP Token to generate OTP codes, the instructions for obtaining and activating this OTP Token can be found in the User Guide.
- Authorisation using an SMS code – the IB Login Password will be provided only to the User in a secure envelope or via an SMS message sent to the Czech mobile operator number designated for the sending of SMS codes.
- Authorisation using a Certificate:
  - the Certification Token will be handed over in person either to the Client or to a person authorised by the Client;
  - a secure envelope with a Certification Centre Login Name and a secure envelope with a Certification Centre Login Password will be provided only to the User.

A Token may not be used by more than one User.

6.6. The Certification Token is used exclusively to store the Certificate necessary for access to IB and for Authorisation of Payment Orders and requests made to the Bank. Users may not use the Certification Token for any other purpose or for storing their own data. For the purpose of the operation of the Certification Token, Clients and Users are obliged to use only the SW provided free of charge by the Certification Centre, and users are obliged to download this SW and save it on their PCs before using the Certification Token for the first time. The Bank shall bear no liability for any damage incurred due to the use of different SW to operate the Certification Token or the use of the Certification Token for purposes other than accessing IB and Authorisation of Payment orders and requests made to the Bank. The Bank shall similarly bear no liability for abuse of the Certification Token due to the use of the default PIN or for damage incurred in connection with such abuse if a User failed to change its PIN immediately after first logging in to IB.

6.7. Clients and Users may contact the Bank in the event that the Token does not function correctly. In such a case, the Bank will arrange for the repair of the Token or its replacement with a new Token. The Bank provides the following warranties for Tokens:

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

- for Clients – consumers, the warranty period is two years,
- for other Clients the warranty period is 6 months.

For Clients who have purchased a Certification Token prior to the effectiveness of these SBC the warranty period is two years.

After the expiration of the warranty period, free of charge replacement of the Token will no longer be possible and in the event of an irreparable defect in the Token the Bank will sell the Client a new Token.

6.8. The Certificate is valid for one year. Users are obliged to submit a request to the Certification Centre for the generation of a new Certificate prior to the expiration of this period. If Users do not request the generation of a new Certificate within the stated period, they will be denied access to IB. Users will also be denied access to IB if they attempt to log in using an incorrect Certificate.

6.9. There is no time limit on the validity of PINs. However, the Bank recommends that Users change their PINs at least once a year. After a specified number of incorrect attempts to enter a PIN the Certification Token will be blocked.

6.10. There is no time limit on the validity of IB Login Passwords. However, the Bank recommends that Users change their IB Login Password at least once a year. Users will be denied IB access after a specified number of incorrect attempts to enter an IB Login Password or an OTP code (when logging in and performing Authorisation using an OTP code) or an SMS code (when logging in and performing Authorisation using an SMS code).

6.11. Renewal of access may be requested by a Client or a User, either in person at a Place of Business of the Bank or by phoning IB Customer Service.

6.12. Clients and Users using IB are obliged, in particular:
- to protect all Security Elements against abuse, loss, unauthorised disclosure and theft,
- to change the IB Login Password provided by the Bank, if Authorisation using an OTP code or an SMS code has been chosen, immediately after logging in for the first time,
- to change the PIN before generating the first Certificate, if Authorisation using a Certificate has been chosen; the SW for operating the Certification Token provided by the Certification Centre must be used to make this change.

6.13. Clients are also obliged to protect their own computer technology system and its components against abuse.

6.14. Clients are responsible for duly securing the IB system against unauthorised access. Clients shall take measures to prevent the abuse of the IB system by third parties.

7. PAYMENT AND BANKING SERVICES PROVIDED VIA IB AND OTHER IB FUNCTIONS

7.1. The main Payment and Banking Services available to Users via IB are as follows:
- Domestic Orders,
- Domestic Bulk Orders,
- Domestic Direct Debit Orders,
- Domestic Standing Orders,
- Intrabank Orders in Foreign Currency,
- Foreign Orders,
- Foreign Bulk Orders.

Users may also:
- view balances on Accounts and the history of Payment Transactions performed on them, if any,
- access Account statements,
- access information relating to payment cards (hereinafter "Cards") issued for CAs to which the Client has access via IB,
- access other data and information available via IB, and send Authorised requests and messages to the Bank.

In IB, Users may also set up notifications to be sent to them regarding Payment Transactions, changes in CA balances etc. (these notifications do not constitute Information within the meaning of the GBC), and may make use of the other available functions of IB.

7.2. The conditions applying to the particular Payment and Banking Services provided via IB are defined in the GBC or respective SBCs; the use of these services via IB and the other available functions of IB are described in detail in the User Guide.

7.3. The Bank may change the scope of Payment and Banking Services provided via IB and the scope of IB functions at any time.

7.4. Where Clients request the express performance of a Payment Order in CZK to an account held with another domestic Provider, they are obliged to indicate this requirement in the relevant IB field when making the Payment Order.

7.5. Clients and Users may contact IB Customer Service in the event of any problems with IB functions, with the Authorisation of Payment Orders and requests made to the Bank or other problems associated with IB.

8. HANDLING OF FUNDS

8.1. Clients are responsible for ensuring that the Funds on a CA are handled via IB only by the Users specified in the Rights and in the manner defined in the respective Authorisation Right.

8.2. Clients are obliged to inform the Bank of any changes in regard to Users, and to request the amendment of the annexes to the Agreement on IB in which such changes occurred. Such amendments will become effective on the next Business Day following the date of the delivery of the duly signed annexes to the Bank, unless agreed otherwise between the Bank and the Client. Clients are liable for any loss or damage incurred due to the breach of this obligation.

8.3. The setting-up of a respective Authorisation Right is an essential prerequisite for a User to be authorised to perform Authorisation.

9. USERS' RIGHTS

9.1. Users may be granted Authorisation Rights with the following scopes:
- **INDEPENDENTLY WITHOUT LIMIT** – a User with this Authorisation Right performs the

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

Authorisation of Payment Orders independently without limitations.

- **INDEPENDENTLY UP TO A SPECIFIED LIMIT** – a User with this Authorisation Right performs the Authorisation of Payment Orders independently up to the amount of a specified Limit. If Payment Orders exceed the specified Limit, Users with this Authorisation Right may only enter them into IB. Authorisation must be performed by a User who has been granted an Authorisation Right with a higher Limit.
- **INDEPENDENTLY UP TO A SPECIFIED LIMIT, BEYOND THE LIMIT JOINTLY WITH ANOTHER USER** – a User with this Authorisation Right performs the Authorisation of Payment Orders independently up to a specified Limit. Payment Orders exceeding the specified Limit must be Authorised jointly with another User.
- **JOINTLY WITH ANOTHER USER UP TO A SPECIFIED LIMIT** – a User with this Authorisation Right performs the Authorisation of Payment Orders only up to a specified Limit, and always jointly with another User.
- **JOINTLY WITH ANOTHER USER WITHOUT LIMIT** – a User with this Authorisation Right always performs the Authorisation of Payment Orders jointly with another User.

An Authorisation Right with a different scope may also be set up following prior agreement with the Bank.

9.2. Users may also be granted Viewing Rights. Users with Viewing Rights are limited to viewing the information available via IB (information relating to Accounts, Payment Transactions performed, Payment Orders entered etc.), and may only enter Payment Orders. The Authorisation of Payment Orders must be performed by a User holding an Authorisation Right.

9.3. In an Authorisation Right, a Client may specify Limits for handling Funds on a CA.

9.4. A Transaction Limit specifies the maximum possible amount of one Payment Order for which Authorisation may be performed. Authorisation may be performed for an unlimited number of Payment Orders whose amounts do not exceed the Transaction Limit.

9.5. A Time-based Limit specifies the maximum possible aggregate value of Payment Orders for which Authorisation may be performed in a designated time period. Authorisation may be performed for an unlimited number of Payment Orders provided that the aggregate amount of all such Authorised Payment Orders does not exceed the Time-based Limit. A Time-based Limit may be set for one Business Day, one calendar week or one calendar month. The Time-based Limit is reduced upon the Authorisation of a Payment Order, and is then reset:

a. at 00:00:01 a.m. each new Business Day, if the Time-based Limit is set for one Business Day. Payment Orders Authorised outside of Business Days are deducted from the Time-based Limit of the next subsequent Business Day;
b. at 00:00:01 a.m. each Monday, if the Time-based Limit is set for a calendar week;
c. at 00:00:01 a.m. on the first day of each calendar month, if the Time-based Limit is set for a calendar month.

9.6. If both a Transaction and a Time-based Limit have been set for an Authorisation Right, both of these Limits must be adhered to at the same time, i.e. Authorisation may be performed for a Payment Order whose amount does not exceed the set Transaction Limit and at the same time does not exceed the Time-based Limit. Therefore, if a Payment Order is within the Transaction Limit but the sum total of all Payment Orders for which Authorisation has been performed to date exceeds the Time-based Limit, Authorisation may not be performed for such Payment Order.

9.7. In the case of Intrabank Orders in Foreign Currency and Foreign Orders (one-time and multiple), the Limit works with the relevant counter-value of the foreign currency in CZK converted using the current Exchange Rate at the time of their Authorisation according to the rules specified in the GBC.

9.8. Payment Orders with a future Maturity Date are deducted from the respective Limits at the time of their Authorisation.

9.9. Clients may arrange for Multiple or Multilevel Authorisation. Multilevel Authorisation may be arranged if the Client has also arranged Multiple Authorisation.

9.10. If Multiple/Multilevel Authorisation is arranged, User Authorisation according to the rules agreed in the Authorisation Right must be arranged for actions performed in IB.

9.11. Users perform the Authorisation of requests, messages and other communications sent to the Bank independently, regardless of the type of Authorisation Right or Viewing Right that has been set up.

9.12. The Client may give a User the following levels of access to information relating to Cards issued on CAs connected to the Client's IB:

- the User will have no access to any information relating to Cards,
- the User will have access to information relating only to Cards where the User is the Card Holder,
- the User will have access to information relating to all of the Cards issued on all of the CAs to which the User has access via IB.

9.13. If the Bank allows IB to be used to submit requests to change or arrange provided services which only the Client has the right to make, the Client may empower a User in the Rights to perform the Authorisation of such requests on the Client's behalf in IB.

10. DATA TRANSMISSION

10.1. Users may use IB twenty-four hours a day, seven days a week. In justified cases, the Bank may interrupt IB service provision, including the acceptance of Payment Orders. The Bank will usually provide advance notice of any scheduled IB service downtime, generally via IB. In the event of technical faults on the part of the Bank or any third party, the Bank may interrupt IB provision without prior notice.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

10.2. In order to access IB, Users must always enter their IB Username and:
- if logging in using a Certificate, enter the PIN for Certification Token and load the Certificate,
- if logging in using an OTP code, enter their IB Login Password and the OTP code,
- if logging in using an SMS code, enter their IB Login Password and the SMS code.

10.3. For Payment Orders manually entered into IB the Maturity Date is required information.
The individual items in one multiple Payment Order imported into IB as a Batch can have different Maturity Dates and their payment can be performed from different CAs connected to IB. If such a multiple Payment Order contains items where the Maturity Date stated has already passed or no Maturity Date is stated, these items will automatically be assigned the earliest possible Maturity Date in accordance with the GBC.
Payment Orders must be Authorised at the latest as of their Maturity Date and within the time period for the submission of Payment Orders stated in the GBC. If the Authorisation of Payment Orders is performed after this time period has expired, Authorisation will either be refused by IB or the further processing of the Payment Orders will be refused after Authorisation.
Additional conditions and the time periods for the submission of Payment Orders and requests to the Bank, their processing, the cancellation of Payment Orders, or for the refusal of a Payment Order by the Bank are set out in the GBC or the respective SBC.

10.4. The only method by which a User may approve the performance of a Payment Order or request made to the Bank is its Authorisation using a Certificate, an OTP code or an SMS code.

10.5. The Bank accepts responsibility only for data received and confirmed by the Bank. The Bank is not liable for any damage incurred due to the incorrect or duplicated entry of data (Payment Orders or requests) via IB.

10.6. The Bank reserves the right to change the manner of submitting data, if required for the secure operation of IB or for other serious reasons.

11. STATEMENTS AND COMPLAINTS PROCEDURE

11.1. Clients are informed of Payment Transactions performed via IB in CA statements delivered in the manner agreed in the respective Agreement on a CA.

11.2. Clients and/or Users are also informed via IB of all currently performed Payment Transactions and of the balance of the Funds on the CA.

11.3. Clients may submit complaints relating to IB via IB itself, via IB Customer Service or at a Place of Business of the Bank.

11.4. The Client consents to the recording of all telephone calls made by the Client or by a User to IB Customer Service, and agrees that the Bank may use such recordings as reference material in any complaints procedure.

11.5. Complaints may be submitted on behalf of a Client by any of its Users.

11.6. Complaints are settled in accordance with these Conditions, the GBC and the Bank's Complaints Code.

12. LOSS, ABUSE, FAULTS AND BLOCKING OF IB

12.1. Clients and Users are obliged to inform the Bank immediately if there is any suspicion of:
- the unauthorised disclosure of Security Elements,
- the potential abuse of IB by a third party,
- a program error and/or an error or abuse relating to the transmission or reception of data.

12.2. Clients and Users are also obliged, as soon as they discover any such occurrence:
- to report the loss or theft of IB service or SW/HW enabling its use (in particular any Security Elements),
- to report any unauthorised Payment Transaction for which they did not submit an order,
- to request, where applicable, the blocking of IB for security purposes.

Such reports may be made in writing, in person at a Place of Business of the Bank, or via IB Customer Service. Where a report is made via IB Customer Service, the reporting person must provide their contact details, via which the Bank will verify the information provided. The Bank may refuse to perform the requested action if it is not possible to verify the information provided.

12.3. Following the making of a report as described above the Bank may block the use of IB. Clients agree to cooperate effectively with the Bank during the performance of corrective measures proposed by the Bank.

12.4. Clients may request the Bank to provide written confirmation that the loss/theft/abuse of Security Elements was reported to the Bank; however, Clients must do so within 18 months of making a report according to Articles 12.1 and 12.2.

12.5. The Client agrees that the Bank reserves the right to block the use of IB in cases including, without limitation to, the following:
- when necessary for serious reasons, in particular reasons of security,
- any suspicion of abuse or attempted abuse of IB,
- any failure to comply with the contractual conditions established between the Bank and the Client, in particular under the Agreement on IB and/or these Conditions and/or the GBC by the Client and/or a User,
- any repeated defects in the operation of IB caused by technical faults in the equipment used by the Client,
- in the cases specified by applicable legal regulations.

12.6. The Bank will inform Clients immediately by telephone or in writing of the fact that access to IB has been blocked, with the exception of any cases where this is contrary to legal regulations.

12.7. In the event that Clients find that access to IB has been blocked, they are obliged to take all necessary steps to unblock or restore their access without undue delay, in order to have access to information about the Payment Services provided to them by the Bank in accordance with the Payments Act.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

13. LIABILITY

13.1. The liability of Clients and of the Bank is provided for in the GBC, these Conditions and the Agreement on IB.

13.2. The Bank is not liable

- for cases where IB cannot be used for reasons beyond the control of the Bank or its partners (interruption of the power supply, interruption of the connection with the Bank via public internet, strikes etc.) including any damage incurred as a result of such cases,
- for damage incurred by a Client due to a breach of the Client's obligations set out in these Conditions,
- for damage incurred due to incorrect Authorisation or any failure to perform a Payment Order for reasons on the part of a Client or on the part of a payment Beneficiary.

13.3. The electronic communications networks (public telephone lines, mobile networks, email and fax) used for communication between the Bank and Clients according to these Conditions are not under the direct control of the Bank, and the Bank is therefore not liable for any damage incurred by Clients due to their potential abuse. The protection of such networks and the confidentiality of messages sent via them must be ensured by the providers of the respective electronic communications services pursuant to legislation including, without limitation to, Act No. 127/2005, on Electronic Communications, as amended.

13.4. The Bank is liable for the functioning of IB, subject to compliance with the Agreement on IB, the Security Principles, the User Guide and any other instructions of the Bank.

13.5. If any malfunctioning of IB for reasons on the part of the Bank is discovered outside of the Bank's Business Hours, the Bank will commence work to rectify such malfunctioning on the next subsequent Business Day immediately after the beginning of the Bank's Business Hours.

13.6. Any and all information regarding the IB system and Payment and Banking Services provided via IB and their use is confidential, and Clients may not use such information in a manner contrary to the purpose for which it was provided to them.

13.7. The Client is also liable for any incorrectly entered data and technical faults on the part of the Client.

13.8. The Client is liable to the Bank for damage incurred by the Bank due to any breach of the Client's obligations under the Agreement on IB, these Conditions or the GBC, or as a result of any incorrect use of IB.

14. TERMINATION OF CONTRACTUAL RELATIONSHIP

14.1. The Bank may terminate the Agreement on IB in the manner provided for in the Agreement on IB and the GBC.

14.2. The Agreement on IB shall similarly expire on the date of the termination of the Agreement on a Client's last CA connected to IB.

14.3. In the event of the termination of the Agreement on IB, access to the Client's Accounts via IB will automatically be cancelled for the Client and all its Users.

15. FINAL PROVISIONS

15.1. These Conditions come into force on 1. 4. 2013 and effect on 1. 6. 2013, as of which date they shall supersede the existing Business Conditions of PPF banka a.s. for the Use of Internetbanking Services effective from 1. 1. 2011.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41, Czech Republic, Company No. 47116129, VAT No. CZ47116129.
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980