Citfin – Finanční trhy, a.s.

Bucharova 1423/6b, 158 00 Prague 13
+420 234 092 011 | info@citfin.cz | citfin.eu

Annex No. 3 to the Framework Agreement

Product Sheet – Payment Services and Spot Trades

This document contains information or refers to additional documents. Its purpose is to specify further the terms and method for fulfilment of the agreement governing the provision of services—specifically the General Terms and Conditions ("GTC") and the Technical Information, both available at www.citfin.cz.

This document contains legally required disclosures that Citfin must provide to the Client under the Czech Payment Services Act (PSA). Citfin will also provide this information in printed form upon request.

Unless otherwise stated, capitalised terms have the meaning defined in the GTC.

Citfin Company Information	**Citfin – Finanční trhy, a.s.,** with its registered office (headquarters) at Bucharova 1423/6b, 158 00 Prague 13, Company ID No.: 25079069, listed in the Commercial Register maintained by the Municipal Court in Prague, Section B, Entry 4313 (**"Citfin"**). Citfin is a company authorised under the CMA, as an investment firm, to provide Forward Trades.
Communication and Provision of Information	Information is provided in the manner and the timeframes stipulated in the GTC. Customer line: +420 234 092 011 Reception: +420 234 092 000 Website: www.citfin.cz Citfin's data mailbox: 7s2n782 All calls related to the provision of payment services are recorded and stored for the period required under applicable legislation, particularly § 31 PSA and § 16 AML Act. Clients also communicate with Citfin through Citfin's internet banking, which serves as a Durable Medium. The Framework Agreement is concluded in Czech. Communication is conducted in Czech. Upon request and subject to agreement, the Framework Agreement and communications may be conducted in another agreed language. However, the Czech version of the Framework Agreement shall always take precedence. During the contractual relationship, Citfin will provide the Client with the full text of the Framework Agreement and its annexes (including the GTC and Product Sheets) upon request.
Communication in Case of Fraud	If Citfin becomes aware of, or suspects, unauthorised or fraudulent use of a payment instrument (e.g., a transaction via internet banking), it shall inform the Client without undue delay by: (i) calling or sending a text message (SMS) to the registered phone number; and (ii) sending an email.
Supervision	Citfin is regulated by the Czech National Bank, Na Příkopě 28, 110 00 Prague 1. Citfin is listed in the CNB register of payment service providers: https://jerrs.cnb.cz.
Protection of Client Funds	Details on Client asset protection are provided in the GTC.
Conflicts of Interest	Information on conflicts of interest and their prevention is included in the GTC.

Client Compensation Scheme	Funds in Citfin's dedicated separate) accounts are covered by deposit insurance in accordance with the laws of EU Member States. In the Czech Republic, coverage is provided by the Financial Market Guarantee System. The deposit insurance limit is currently set at EUR 100,000. It applies to the sum of all funds per Client per single institution. The Client acknowledges that under the law, certain individuals may not be eligible for compensation. More information is available at www.citfin.cz.
Payment Services Provided	**Citfin provides the following payment services:** a) Execution of Spot Trades (purchase or sale of one currency against another); b) Establishment of Client Payment Accounts (CPA) to enable the transfer and receipt of Client funds in CZK and foreign currencies to/from other bank accounts; c) Provision of internet banking services; d) Provision of Phonebanking services; e) Provision of the Client API service linked to the CPA; f) Provision of the Citfin API service. **Purpose of the Client Payment Account (CPA)** The PÚK is used for: a) recording funds entrusted by the Client to Citfin; b) executing and recording Payment Transactions; c) executing and recording Exchange Trades; d) recording Collateral Value in relation to Forward Trades if such arrangement is in place. **Spot Trades** The Client may enter into the following Spot Trades with Citfin: a) **Spot Trade** – purchase or sale of foreign currency with settlement typically within 2 Business Days. – Settlement may take up to 4 Business Days in the following cases: – if the transaction is in EUR and involves a currency exchange between EUR and a non-EEA currency within the EEA; – if the transaction is in CZK but is executed outside the territory of the Czech Republic; – if the transaction involves an EEA currency other than EUR; – if Citfin as a provider to both the payer and the recipient of payment services provides payment services in an EEA member state and the transaction is in a non-EEA currency; – if only the payer or payee provider operates in the EEA and the transaction is in a non-EEA currency; – if both the payer's provider and Citfin as the recipient's provider provide payment services in an EEA member state, and the payment transaction is executed in a currency that is not the currency of an EEA member state, payment services in an EEA member state are provided only by the payer's provider or only by the recipient's provider. b) **Order** – an instruction to enter into a Spot Trade when the agreed rate is reached (or as close as possible to it, given market conditions). – Take Profit Order – an instruction to automatically buy/sell currency at the Client's requested rate. For example, with the purchase of a foreign currency the Order must be placed at the current market rate. – Stop Loss Order – an instruction to automatically buy/sell currency at a Client-determined worst-acceptable rate. For example, a buy Order is placed above the current market rate. – Combination of TP and SL Orders – both Orders may be placed simultaneously.
How Spot Trades Are Executed	Spot Trades are executed: via Citfin's Dealing Desk, or via Citfin's internet banking, in accordance with the GTC and the Technical Information. The GTC also contains a more detailed description of the abovementioned payment services. **Online Trading Procedure for Spot Trades** Agreement of a Spot Trade as part of the Online Trading service in internet banking takes place as follows: Via internet banking > "Online Trading" tab: a) The Client selects trade parameters: – Currency sold;

	– Currency bought; – Amount (in sold or bought currency); – Settlement date: – T+0 – same Business Day (must be placed before the relevant cut-off time listed at www.citfin.cz); – T+1 – next Business Day; – T+2 – second Business Day. b) After filling in the abovementioned parameters, the Client requests a quote, i.e., for the currently offered Spot Exchange rates for the said parameters. c) The offered Spot Rate is displayed. The Client has 5 seconds to accept the quote. If not accepted within 5 seconds, the trade is not concluded. If the Client clicks "Confirm Trade", the trade is concluded based on the selected parameters and the offered rate. A Confirmation is then issued as per the GTC.
Fees and Costs Related to Services	Fee information is available in the Framework Agreement and the applicable Fee Schedule.
Exchange Rates for Spot Trades	Citfin applies current rates valid at the time of Spot Trade settlement, or, for Orders, at the time of execution. Citfin's rates derive from current exchange rates and are based on quotes received from its liquidity providers (cooperating financial institutions) at which the exchanges are subsequently settled. Citfin applies a spread of 0–3%, depending on: trade volume; the Client's total exchange turnover; servicing costs; market conditions; and other relevant factors.
Requirements for Executing Payment Services	The formal requirements, procedures for submitting Payment Orders, and the timing of their receipt and acceptance by Citfin are defined in the Technical Information.
Interest on Client Funds	Funds held by Citfin in the Client's CPA for the purpose of executing Payment Transactions or Spot Trades are not interest-bearing.
Execution Times for Payment Services	See below.
Payment Instruments and Responsibility for Unauthorised or Incorrect Transactions	Information about the issuance of payment instruments, liability conditions for losses resulting from Unauthorised or Incorrect Payment Transactions, and the corrective settlement process (e.g., information on terms for correction of accounts) is provided in the GTC and the Technical Information.
Communication in Case of Loss or Theft Protection Measures for Payment Instruments	The Client is obligated to contact Citfin immediately in cases of loss, theft, or suspected misuse of: verification devices; access credentials (PIN or Client ID); or tokens generating a Verification Code; the Client, in case of any unauthorised or incorrect execution of a payment transaction, must immediately notify Citfin via: – phone: +420 234 092 000; – email: info@citfin.cz. Citfin will block the Verification Device or access password without delay and no later than the next Business Day following receipt of the report. **Protection of Payment Instruments** When using internet banking, Phonebanking, or any other payment instrument, the Client must adhere to essential security principles. Failure to do so may result in liability for resulting losses. Access to Citfin's internet banking and Phonebanking services is granted only through secure personal authentication tools: client ID; PIN; Verification Device (to which a Verification Code is sent) Token, generating a Verification Code (**"personal security features"**). Compliance with the security rules set out below is essential for Citfin to prevent or minimise misuse, in particular the execution of unauthorised payments. Unintentional violation of these security rules constitutes a breach of the Client's obligation to use the payment method (Phonebanking, internet banking) in accordance with the agreed terms and conditions due to gross negligence, and Citfin shall not be liable for any damage caused by such misuse.

Key Security Measures (Client Responsibilities)

- Personal security elements are non-transferable and may only be used by the designated individual.
- If sent by mail, devices must be checked for tampering. Refuse damaged packages and ask the deliverer (courier) to write a protocol on the damaged package. Report this to Citfin immediately.
- PIN codes can also be delivered in person or via a Citfin dealer (trader).
- We issue PIN codes sole for the purpose of their use for Phonebanking and online banking. If used for a different purpose, Citfin bears no liability for said use.
- PIN codes sent by Citfin serve only for initial long to online banking. The PIN must be changed upon first login.

Carefully protect your personal security features against loss, theft, misuse, and any use by another person. Under no circumstances and in no way may personal security features be provided to another person. At the same time, we ask you to prevent any alteration or other unauthorised intervention that would change the nature, purpose or character of the issued personal security feature (PIN). In your own interest, please inform us immediately of any loss, theft, misuse, or unauthorised use of personal security features (PINs) in the manner described above.

In your own interest, always carefully adhere to the following security rules, which are essential for your protection against misuse of internet banking. If you do not follow them, we cannot adequately protect you, especially against unauthorised fraudulent payments:

- Always log out of internet banking as soon as you finish using it.
- Do not choose a PIN that is simple and can be deduced from your identification details.
- Do not store your PIN in an easily readable and accessible form and do not allow it to be remembered by your internet browser.
- Change your PIN regularly (at least once every three months) and protect it from disclosure.
- Do not access online banking using technical equipment that is publicly accessible (e.g., from a computer in an internet café) or that you are not familiar with.
- Do not access internet banking using technical equipment (e.g., a mobile phone) that can also be used by other people to access internet banking.
- Do not allow other people to register their biometric features on your devices or applications.
- Always use your own technical equipment or our technical equipment, or equipment whose security you have reliably verified before use.
- Never use technical devices or software whose security is in any way questionable.
- Do not open emails or email attachments from suspicious senders or messages with suspicious names or content.
- Do not reply to or otherwise respond to such emails.
- Do not visit risky websites on the device you use for online banking.
- Do not open links to unknown servers on the internet or those found in suspicious emails.

Do take the following precautions

- Use spam protection for your email inbox.
- Always use the latest versions of operating systems, security programmes (antivirus, firewall, etc.) and internet browsers supported by the manufacturer on your technical devices.
- Only install and use programmes from trusted and previously verified sources that do not contain malicious code on your technical devices.
- If possible, set your phone to prohibit installation from unknown sources.
- Always enter your personal security details only on the websites www.citfin.cz or www.bankservis.cz, or in the applications of authorised providers of indirect payment order services or in the applications of authorised providers of payment account information services.
- Before entering them, always carefully verify that you are on these websites or that you are using an application of an authorised provider of indirect payment order services or an authorised provider of payment account information services.
- Always launch internet banking only from our website or by entering bankservis.cz in the address bar of your browser or from a link sent by us. Do not search for this page using a search engine or launch it from your favourites tab.
- After logging into internet banking, always first carefully read any warnings about current threats and risks posted on our website or in internet banking and always comply with the obligations specified therein.
- If, after reviewing them, you identify any imminent risk to the security of your access to online banking or your Client Account, immediately log out of the application and contact us at the number above.

Follow the same procedure in any other case where you suspect that the security of your access to online banking or your Client Account is compromised. Before logging in and throughout the entire time you are logged in to online

	banking regularly check that the address bar properly shows https://bankservis.cz. Click on the lock icon to make sure that the secure connection certificate was issued for bankservis.cz.
Technical Information (Requirements)	Information on required client-side equipment and software is available in the Technical Information.
Changes and Termination of the Framework Agreement	Citfin may amend the Framework Agreement or GTC under the procedures stated therein. If changes to the Framework Agreement or the GTC are announced at least two months in advance and the Client does not object prior to the date of their entry into force, the changes are deemed accepted. The Framework Agreement is concluded for an indefinite period. Either party may terminate or withdraw from the Framework Agreement in accordance with the terms of the Framework Agreement and the GTC.
Governing Law and Dispute Resolution	Governing law, dispute resolution procedures and options for out-of-court settlement are stipulated in the Framework Agreement and the GTC.

Settlement Timeframes for Domestic and Foreign Payments

The following tables show the cut-off times for processing Payment Orders and posting funds to the CPAs as required by the GTC and Technical Information.

NORMAL Payment Speed Cut-off time for accepting orders and crediting funds to the CPA for same-day settlement	
Currency	Cut-off Time
All Citfin-supported currencies	16:30

URGENT Payment Speed Cut-off time for accepting orders and crediting funds to the CPA for same-day settlement	
Currency	Cut-off Time
CZK – domestic	12:30
CZK – cross-border	11:30
EUR – within EEA	15:00
EUR – outside EEA	15:00
USD	14:00
GBP	13:30
CHF	08:30
NOK	08:30
SEK	08:30
JPY	not supported
PLN	08:30
CAD	14:00
HUF	13:30
DKK	08:30
AUD	not supported
RON	not supported
CNY	not supported