Cash Management User Guide

Hungary

Treasury and Trade Solutions

citi

Table of Contents

I. Introduction

Thank you for choosing Citi's Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this Cash Management User Guide (User Guide) is to provide Customers with a manual containing detailed information of Services available to Customers and is to be read together with your Account Terms, Pricing and Cut-Off Times Schedule.

The Pricing and Cut-Off Times Schedule means information on the pricing of available Services, which is available on the Bank's website and contains the rates, charges and other fees and cut-off times applicable to the Bank's Services.

In this Guide, Citi and Bank may be used interchangeably, and in each case refer to the following Citi entity:

Citibank Europe plc Hungarian Branch Office (registered office: 1051 Budapest, Szabadság tér 7., registration court and court number: Municipal Court of Budapest, acting as Court of Registration 01-17-000560) acting in the name and on behalf **Citibank Europe plc** (registered office: 1 North Wall Quay, Dublin 1, registration court and court number: Companies Registration Office, no. 132781) an entity registered in Ireland.

This Guide may be updated from time to time and any change will be communicated through our regular channels.

The Bank's procedure for amendments:

1. The Bank follows the provisions of the Local Conditions in making amendments.
2. The Bank informs the Customer of changes to the Terms in writing at least 2 months in advance of the amendment taking effect.
3. If the Customer does not agree to the suggested amendments, the Customer can terminate the Terms immediately and free of charge, but not later than the date the amendment takes effect.
4. Lack of termination from the Customer is considered its acceptance of the proposed amendments.

Information on demand: The Bank will provide the Customer with a copy of the Terms and information specified in Section 10 of the Hungarian Payment Services Act (including the list of items specified there) on paper or on another durable medium at any time upon the Customer's request.

II. Payment Services

A. Types of Payments Services in Hungary

- Internal Transfers: Transfers of funds to another customer's account or between the Customer's own accounts within the Bank in Hungary.
- Automated Clearing House (ACH) – HUF Transfers via GIRO: Domestic electronic funds transfers used to deliver funds to an Account at a non-Citi financial institution from a Citi account through the local clearing house in HUF. HUF ACH provides 10 intraday clearing cycles to clear HUF interbank payments.
- Real-Time Gross Settlement (RTGS) – HUF Transfers via VIBER: A large-value funds transfer system based on continuous settlement of payments on a gross, individual order basis. VIBER is a SWIFT-based system mostly used by investors and financial institutions.
- Direct Debits: A means of collecting monies owed by a payer, where the payee ("originator") generates the initiating transaction to be processed by the payer's bank against the payer's account. The two main types of HUF direct debit solutions in Hungary allow initiating requests for direct debit against the Customer's HUF account(s):
    - Collection Based on a Proxy Letter: In the power of attorney (proxy letter) the payer (Customer) gives consent, in the manner notified to the payment service provider, to the payee to execute the direct debit payment transaction. The proxy letter also may lay down conditions (e.g. upper limit of payment or the period of queuing in the event of insufficient funds or validity period for the authorization) for submission if so agreed between the payer and his payment service provider.
    - Automatic Debit Transfer (Group Collection): By authorization of the payers concerned, if agreed between the payee and payment service provider carrying his account, the payee shall submit direct debit requests of the same title codes for the transfer of sums from the payment accounts of a large number of payers on a specific debit day, grouped in batches. This type of direct debit is typically used by utility companies to collect their monthly bills. This collection type also requires a Proxy Letter to be in place to regulate maximum collectable amount.
- Cross Border Funds Transfers: Allow Citi customers to make international transfers in a wide range of currencies as outgoing transfers.
- SEPA Payments: Payments in euros to an account within the Single Euro Payments Area (SEPA). SEPA is euro clearing mechanism for low-value, high-volume payments, which include both a mandate-based direct debit service and a credit transfer service for individual, bulk, and same day, or a combination of bulk and same day, credit transfers.
- SEPA Payments – Bulk: SEPA outgoing payments from the Customer's payment account debited in one bulk amount, which equals the sum of individual SEPA outgoing payments.

- SEPA Direct Debits: Payments in euro made from the Customer's payment account at the request of the payee within the SEPA Area.

B. Sending a Payment

1. The Customer sends a payment instruction to Citi, formatted to market standards and as outlined at the time the payment service was implemented, via:

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM"), TreasuryVision®, and WorldLink®)
- CitiConnect®
- Email/fax with the Bank excluding Manually Initiated Funds Transfer (MIFT) - refer to Section V for details on initiating manual transactions

CitiDirect BE® is an electronic banking platform (available via web, tablet and mobile) that provides one-click access to global transaction capabilities using an intuitive and user-centric workflow. CitiDirect BE® supports multiple transaction types across multiple geographies, subsidiaries, and currencies. Users can originate communication such as enquiries, data and other information exchanges, advices, transactional instructions, and account management instructions.

CitiConnect® provides the Customer an electronic banking platform to streamline its file exchange and messaging processes, reduce costs using automated processing, and expedite dispute resolutions associated with the Customer's cash management needs. CitiConnect® integrates banking execution and information with the Customer's enterprise-wide treasury management, ERP and other cash management systems.

Further information on the use of the above banking platforms can be found in Section VI (TTS Consolidated Security Procedures) and on the Bank's Channel Services website: https://www.citibank.com/tts/solutions/channel_services/index.html.

2. The Bank only accepts payment orders that conform to the Bank's requirements, or that are given on a special form used by the Bank for this purpose. Payment orders that deviate from this requirement may be refused by the Bank by giving a notice to the Customer to that effect.

3. The Customer initiates payment orders and submits them to the Bank in accordance with the Cut-Off Times Schedule. Any payment orders received by the Bank after the specified cut-off times are considered to be received on the following banking business day. Payment transactions, except official transfer orders and court transfer orders, are executed upon the payer's approval (i.e. valid signature of the Customer's authorized representative, sign-off granted in the electronic system in accordance with system characteristics and the Customer's system specifications, or a valid direct debit authorization letter approved by the payer's bank).

4. The Customer may withdraw or modify in writing certain payment orders before the Account is debited. All costs and consequences of the withdrawal or modification of a payment order will be at the expense of the Customer.

The procedure for modifying, cancelling or recalling orders received by the Bank is as follows:

a. The Bank accepts duly signed, written orders as per the Signature Mandate for modification, cancellation and recall.

b. The Bank credits an order's amount upon its return from the beneficiary's bank, or in case of in-house bank transfers after the payee grants its contribution for recalling, on the value date of return and consent, after the deduction of fees and with the exchange rate difference used by the beneficiary's bank in case of conversion.

c. The Bank accepts modification, cancellation and recall requests provided they include all the original transaction data.

5. The Bank is not able to modify the following orders:

   a. Transfer orders via the GIRO system and internal book entry transfers within the Bank;

   b. Any VIBER transfer orders already entered in the books and approved by the Bank;

   c. Standing payment orders (in case of a change, a new standing order must be submitted);

   d. Orders, with respect to the execution of which the Bank issued a confirmation of execution;

   e. Transactions carried out with bank cards.

6. Citi forwards the instruction to the relevant payment system for further processing.

7. The payment system forwards the instruction to the beneficiary bank based on the locally defined clearing cycle.

8. The beneficiary bank credits the beneficiary account.

9. The Customer may initiate the correction of the not-approved or approved, but wrongly executed payment transaction, within 90 days commencing from the fulfilment of the payment transaction. The Bank shall promptly investigate the request for correction and fulfil the request for correction depending on its result.

10. Except for the corrections as set out in the previous point, the Bank does not provide reimbursements for the Customer for payment transactions initiated by or through the beneficiary and approved by the Customer.

C. Receiving Direct Debits (Payments)

Citi, as the Customer's paying Bank, supports incoming requests for Collection Based on a Proxy Letter (in HUF) and Automatic Debit Transfer (in HUF) from other participating financial institutions or partner banks.

SEPA Direct Debits: Payments in euro made from the Customer's payment account at the request of the Payee within SEPA.

Direct Debits in Foreign Currencies (FCY): Payments in FCY made from the Customer's payment account at the request of the payee.

1. Citi validates the transaction received against the direct debit mandate (or equivalent) previously communicated by the Customer to Citi before payments are made.
2. If the direct debit payment is in compliance with the direct debit authorization, Citi processes the instruction and debits the Customer's account.
3. In the event there is no direct debit authorization or are insufficient funds in the Customer's account, Citi will not process the direct debit payment and sends the unsuccessful debit status back to the direct debit payment system or partner banks.

Citi will reverse any entry passed erroneously and debit or credit the relevant Account.

D. Cash Withdrawals

Citi offers the Customer a range of cash withdrawal solutions for physical notes and coins:

- HUF banknote and coin withdrawal at Citi's Cash Centre
- HUF banknote and coin withdrawal in bag (by a Cash Transporter Company)
- Foreign currency banknote withdrawal at Citi's Cash Centre
- Foreign currency banknote withdrawal in bag (by a Cash Transporter Company)

Cash Withdrawal and Collection Process using Cash Transporter Company

1. The Customer concludes an agreement directly with the service provider (which is in contractual relationship with the Bank) of its choice.
2. Prior to the first delivery/pick up, the Customer submits to the Bank a duly signed Proxy Letter in which the Customer certifies that the Cash Transporter is authorized to transport in its name. If the service provider changes, the Customer must submit a new Proxy Letter.
3. The Customer submits in advance an original of the designated Cash Withdrawal Slip by fax, on which Customer can specify its possibly denomination request. If the Customer does not indicate its denomination request on the form, the Bank shall package the requested amount in such denominations as are available.
4. The Bank or its contracted cash processing organization (in the absence of the Customer) packages the quantity of cash and respective denominations intended for withdrawal, and hands it over to the Cash Transporter or Customer or its authorized representative.
5. In case of deficiency or suspicion of the authenticity or originality of the documentation or persons involved with the cash withdrawal and transportation process, the Bank will not hand over the consignments. In such cases, minutes will be made by the person proceeding on behalf of the Bank and the person proceeding on behalf of the Customer or Cash Transporter. They will record the time and place of the cash withdrawal attempt and all the circumstances leading to the refusal to fulfil the order. The minutes will be

authenticated with the signatures of the person proceeding on behalf of the Bank and the person proceeding on the behalf of the Customer or Cash Transporter.

6. The Bank places the cash, packaged into cash transportation bags provided for this purpose, and closes the bag with a seal.
7. If the bag or documentation does not conform to the above guidelines, the Customer or Cash Transporter does not have to accept the transportation bag.
8. If the Customer collects cash directly from the Bank, the cash will be handed over upon receipt of the original cash withdrawal order signed by the Customer and verification that the individual collecting the cash is authorized as set out in the Bulk Cash Withdrawal Request Form. If the Cash Transporter is collecting cash on behalf of the Customer, the Bank will validate that the employee of the Cash Transporter is authorized per the agreement between the Cash Transporter and the Bank.
9. Packaging of banknotes and coins takes place in the Customer's absence, on the premises of the Bank or the cash processing organization contracted by the Bank, under video surveillance. Video recordings are retained by the Bank for a period of one month. If the Customer detects a discrepancy within seven days following the day of the cash handover to the Customer or its agent, the Customer must notify the Bank of the discrepancy for review. The Bank will refer to video surveillance to investigate the matter.

Cash Withdrawal at Citi's Cash Centre

The Bank offers over-the-counter services at Citi Cash Centre (1134 Budapest, Huba u. 2-4), where the Citi's Customer or its representatives can withdraw cash from its accounts on banking days. Service available for:

- Customers who act on their own behalf and for their own benefit.
- Customer's representatives based on mandate.

E. Payroll Accounts

Citi offers payroll account for managing payroll transfers separately and confidentially.

1. The Customer may open a Payroll Account at Citi Hungary.
2. The Customer provides the Bank with an address and a list of persons to whom the Payroll Account statements shall be sent. The Bank, based on the Customer's payroll transaction submission, transfers from the Customer's main account to its Payroll Account, which are kept in the same currency, the coverage for payments from the Payroll Account on the value date of such payments, provided there are enough funds on the Customer's main account. The payroll account also may be funded directly by the Customer on the same day as scheduled payroll payments.
3. At the end of the payroll day, the Bank transfers any excess funds from the Payroll Account to the main account.

F. Non-Refundable Housing Loan Assistance Account

Citi offers Non-Refundable Housing Loan Assistance Account for the purpose of segregating the amounts of housing loan repayment assistance and non-repayable housing assistance granted to the Customer's employees as a Cafeteria benefit.

1. The Customer may open a Non-Refundable Housing Loan Assistance Account
2. The Customer provides the Bank with an address and a list of persons to whom statements of the Non-Refundable Housing Loan Assistance Account shall be sent.
3. The Customer, at its own liability, submits transfer orders for debiting the Housing Loan Assistance Account in compliance with sections 2.7 and 9.3 of Annex 1 of the Act on Personal Income Tax.
4. The Customer indicates the following data in the comments field of the order for any transfer transaction launched from the Assistance Account:
    - Name of the individual receiving the assistance;
    - Tax ID of the individual receiving the assistance;
    - Title of the assistance (home loan repayment assistance or non-repayable housing assistance granted as a Cafeteria benefit);
    - Any other such data, relating to the individual receiving the housing assistance or to the provider of the assistance that the Bank is required to indicate in its data reporting.
5. The Customer will reimburse the Bank for any tax payment obligations (including the amount of any tax fines or default penalties) and any additional costs, arising from the reporting of incomplete data or the failure to report data to the tax authority due to the Customer's failure to provide the data, for which the Bank has no responsibility.
6. The Bank transfers the coverage for payments from the Non-Refundable Housing Loan Assistance Account on the value date of such payments from the Customer's Main Account kept in same currency as the Non-Refundable Housing Loan Assistance Account by the Bank provided there are enough funds on the Customer's Main Account. The Non-Refundable Housing Loan Assistance Account also may be funded directly by the Customer on the same day as scheduled payments.
7. The Bank transfers all amounts left at the end of the day on the Non-Refundable Housing Loan Assistance Account or received from third parties to the credit of the Non-Refundable Housing Loan Assistance Account to the Main Account with the same value date. In this case the Customer authorizes the Bank to use incoming amounts to the Non-Refundable Housing Loan Assistance Account on the day of the payments from the Non-Refundable Housing Loan Assistance Account for that day's payments.

G. Electronic Bank Message Module (EBÜK) Service for Customs and Non-Community Taxes and Fees Payments

1. The Customer authorizes its representatives, prior to the use of the Service using the Bank-provided form and downloads the certificates related to the Service via CitiDirect BE®. The Customer also provides to the Bank, in writing, the customs ID applied to transfers launched in favor of the National Tax and Customs Administration (NAV) as the beneficiary.

2. The Bank will only send messages to NAV's system with regard to irrevocable transfer orders that have been accepted in favour of the public finance income accounts published by NAV.

3. The Customer defines the HUF payment account to be used for the purpose of the EBÜK Services.

4. The Customer initiates the transfers via the CitiDirect BE® system. Citi then forwards notices related to the Bank's transfer of customs and non-community taxes and fees via the National Tax and Customs Administration (NAV) of Hungary's EBÜK system.

5. Citi will certify to NAV, within an hour that public dues have been paid.

6. Transfers are initiated via CitiDirect BE® system either by uploading or manual entry, as a "Domestic HUF Transfer". The following data should be included in a transfer initiation or the transfer may be rejected:

   a. Beneficiary's ID: EBÜK code + VPID

   b. Actual beneficiary's name and address: Line 1 – Name; Address

   c. Actual beneficiary's name and address: Line 2 – Address continued

   d. Actual beneficiary's ID: Resolution number + tax number or tax ID related to the VPID.

   e. Reference to the "EBÜK/EBUK" Service in the order.

   The absence of above mentioned specific data related to the Service does not affect the execution of a Domestic HUF transfer submitted successfully to the Bank.

7. Within 1 business day, the Bank issues an EBÜK transfer 'Certificate' addressed to the Customer in html format, which can be downloaded via CitiDirect BE®. The certificate includes data passed through the EBÜK system to the NAV and details the cost of the transfer.

H. Resolving Unauthorized Transactions

The Customer may request the Bank to remedy any unauthorized or incorrectly executed payment transaction within 90 calendar days after its execution.

Unless provided otherwise in the Terms or by applicable regulations the Bank follows the below procedure when it becomes aware of an unauthorized payment transaction debited on the Customer's Account.

The Bank immediately:

a. Refunds to the Customer the debited amount;

b. Restores the Account to its original (pre-debit) status; and

c. Provides compensation to the Customer.

I. Incorrectly Executed Payment Transactions in the European Economic Area

The Bank will refund to the Customer any incorrectly executed debit transactions unless the payment is debited on the account of the payee's payment service provider, in which case the payee's payment service provider shall immediately credit the payment on the payee's account.

The Bank will immediately re-submit the Customer's payment order to debit a third party's account (direct debit order) if the Bank is informed that the order was not correctly transmitted the first time. The Bank will process the incoming payments in line with the applicable regulations and will credit such amounts on the Customer's account immediately after the amount is credited on the Bank's account.

Upon the Customer's request the Bank will immediately make every reasonable effort to investigate the unexecuted or defectively executed payment transactions and will keep the Customer updated about its findings.

III. Receivables Services

A. Receiving a Payment

1. The clearing system forwards the instruction to Citi based on the locally defined clearing cycle.

2. Citi credits the Account.

   Any rejections or returns by Citi will be credited back to the payer account. The reason for the return is communicated to the payer.

3. Processing of incoming items.

The Bank processes transactions that arrive at the Bank according to Cut-Off Times Schedule, provided that all information necessary for crediting the amount on the beneficiary's account has been duly provided. For amounts reaching the Bank after the defined cut-off times, the Bank will deem the amounts to be received on the next business day and process them the next business day.

The Bank's cut-off times for submitting orders for same-day processing and for fulfilment of orders are available in Cut-Off Times Schedules.

B. Automatic Debit Transfers (Group Collections)

A direct debit collection is a financial transaction originated electronically by instructing the Bank to withdraw funds from a payer's bank account.

Direct Debit Collection Setup and Mandate Management

1. Prior to start the Service the Customer must submit GIRO Collector ID registration form together with signing a Group Collection Order Form. GIRO registration must be forwarded to GIRO by 14th calendar day of a month in order to validate the Collector ID as of the next month.

2. The Bank receives and stores mandate files containing the data related to the Customer's authorizations via the GIRO system.

3. The Customer ensures that its payers provide the necessary authorization to their bank for the acceptance of the group collection orders initiated by the Customer.

4. The Customer must have opened a designated account for the Service.

5. The Bank converts the mandate files into .dda format, and compiles a daily bulk file of authorization messages sent to the Customer's Collector ID via CitiDirect BE®. The Customer completes the .dda file in accordance with GIRO standards and the specifications provided by the Bank, and returns it with an .ext extension to the Bank via electronic mail (hereinafter: e-mail), using the encryption method stipulated by the Bank, to a designated e-mail address. When the Bank stipulates the use of specific encryption software, the Customer purchases such software at its own cost. Before the Customer returns the authorization messages to the Bank, and if required due to the encryption

software, the Customer and the Bank conduct an exchange of keys to ensure that the Bank can decode the data sent by the Customer to the Bank.

Direct Debit Collection Process

1. The Customer initiates the transaction and sends the instruction file to Citi and/or uploads files/reports via the agreed Citi e-banking channel.
2. Citi validates that the transaction request contains all required information.
3. Citi sends the direct debit transactions to the receiving payer banks via the clearing system.
4. Citi credits the funds to the Customer's account within the agreed time (subject to the Bank's receipt of the funds), and prepares reconciliation reports, provided that all necessary data is duly available.
5. The Bank decodes the .ext file sent by the Customer, converts it into the GIRO format and forwards it to the obligors' banks.
6. The Bank examines authorization messages contained in the .ext file exclusively from an information technology point of view, not with regard to their content. If the Bank encounters erroneously completed authorization messages, it will attempt to correct the file. Should such efforts fail, the Bank notifies the Customer of the error, and the Customer then resends the corrected file.
7. The Customer ensures that authorization messages are sent within the time frame provided in the operating regulations.

C. Refunding debit transactions initiated by the payee (direct debit)

Upon the request of a micro-enterprise Customer the Bank will refund authorized direct debits booked on its Account and paid to a payee situated in the European Economic Area if it is verified that the Customer was unaware of the exact amount of the direct debit and this amount was higher than the Customer could have reasonable expected. At the verification of the refund request the Bank will consider the Customer's previous transaction history and any other relevant circumstance. The Customer may request such refund within 56 days after its booking.

The Bank will either refund the direct debit within 10 business days or provide justification for not complying with the Customer's request.

D. Cash Collection

Citi offers customers a range of cash collection solutions for physical notes and coins:

- HUF banknote and coin deposit at Citi's Cash Centre
- HUF banknote and coin deposit in bag (by Cash Transporter Company)
- Foreign currency banknote deposit at Citi's Cash Centre

- Foreign currency banknote deposit in bag (by Cash Transporter Company)

Cash Collection Process using a Cash Transporter Company

1. The Customer concludes an agreement directly with the service provider of its choice which is in contractual relationship with the Bank.
2. Prior to the first delivery, the Customer submits to the Bank a duly signed Proxy Letter certifying that the Cash Transporter is authorized to transport and process cash in its name. If the cash transport service provider changes, the Client must submit a new Proxy Letter.
3. The appointed service provider picks up physical cash from the Customer's designated location(s) on the day specified in the mutual agreement. The Customer counts the cash and places it in a tamper-proof self-seal plastic bag with a paying-in slip (deposit slip) provided by the service provider.
4. The cash is inspected for defective, counterfeit or unacceptable notes and counted. The authenticity and condition of the currency notes and coins is verified by the service provider. The Bank credits the Customer's account(s) based on the report received from the service provider in a way determined in the agreement concluded between the Bank and the Cash Transporter and in accordance with the internal control policies of the Bank.
5. The service provider representatives transport the collected and processed cash to the cash counting centre designated by the Bank.
6. Currency notes or coins found to be counterfeit will be dealt with according to applicable laws and regulations; any related costs or consequences are the Customer's responsibility.

Deposit at Citi's Cash Centre

The Bank offers over-the-counter Services at the Citi Cash Centre (1134 Budapest, Huba u. 2-4), where the Customer can deposit cash to its accounts on banking days. Services are available for:

- Customers who act on their own behalf and for their own benefit
- Customer's representatives, based on mandate.

If the amount of a deposit is more than HUF 10 million (or equivalent in foreign currency), based on the order of NBH 19/17 15.§ (3), the Customer must declare the source of the funds.

E. Postal Money Circulation Services

The Customer can apply for Postal Cheque solution using the designated form. The Service will be provided until the designated account for the Postal Cheque Service is opened. Postal Cheques are pay-in slips in a standard format specified by the Post Office (Posta) and include an Optical Character Reader (OCR) strip at the bottom. The Customer can

customize these slips to include data about the Customer's Citi account and details of a receivables item. After customization, the cheques can be sent to the Customer's partners, who can then use them for making cash payments at any of the post offices in Hungary. The payments are processed by the Postal Clearing Centre and then credited as an aggregate amount to the Customer's bank account. Citi provides the Customer detailed payment data broken down by postal settlement days for reconciliation on paper or CitiDirect BE® (HTML or ASCII file). Citi also supports cheque embossing.

The Postal Cheque solution relies on the Services provided to the Customer by Posta. As such, Posta is to be contacted for any inquiries and claims related to its Services, or any delays or errors resulting from these Services, except for printing of Postal Cheques ordered via the Bank.

If the Customer assigns a payer ID to its partners using Postal Cheques, the Customer must ensure that the payer ID is indicated on the Postal Cheque. When making the request, the Customer must select how data should be forwarded from the following options:

- On paper, in the form of a printed letter, or
- Via the CitiDirect BE® system in the form of a displayable and printable electronic letter (HTML), or
- Via the CitiDirect BE® system in an electronic data file (ASCII file).

Based on the Customer's request, the Bank orders, on behalf and in place of Customer, the production of the Postal Cheque form from Posta and/or the classification by Posta Settlement Centre of sample copies of the forms, and informs Customer of the result.

F. Payer ID Account (Speed Collect Buyer ID)

The Citi Payer ID Account (also called Speed Collect Buyer ID) solution offers a reliable way of identifying payers for incoming payments through the CitiDirect BE® platform. The solution is available for domestic transfers. The purpose of the Service is to provide the Customer special electronic account statement information, called SpeedCollect Buyer ID Information, which also contains an 8-digit reference number in file format. A SpeedCollect reference number is added to the Customer's GIRO account number for the Customer's incoming funds transfers to facilitate the identification of such transaction by the Customer to its counterparty.

1. The Bank communicates to the Customer a set of Payer ID numbers that the Customer can use to represent the Customer's Account.
2. The Customer attributes and communicates the Payer ID(s) to the payer(s) of its choice.
3. The payer initiates a payment in favor of the Customer quoting the Payer ID.
4. The Bank credits the payments and generates report. The Buyer ID will be displayed separately on the bank statements, which can be downloaded electronically from CitiDirect BE® platform. Bank stores this account statement information for a period of 3 months.

IV. Other Considerations

The Customer will make its own assessment of the legal, regulatory, tax and accounting implications of the Services.

From time to time, the Bank shall deliver to Customer fee schedules, procedures, requirements, guides, manuals and other materials describing the procedures, requirements and limitations surrounding the use of the Services.

The clearing of payments and receivables is governed by the rules set by the corresponding clearing system. Both Citi and our Customers must adhere to these clearing rules.

Any changes to company documentation, representatives, signers and beneficial owners, as well as their respective details, are to be reported to the bank within 5 working days by the client. Based on these reported changes, the Bank updates its records that are then used in accordance to Hungarian AML Act.

V. Manual Initiation of Instructions

Citi offers its Customers the ability to initiate manual instructions or Manual Initiated Funds Transfer (MIFT) in the event of a contingency or other scenarios that may involve a manual instruction, including amendment, recall or cancellation of previous instructions. Specific country regulations may apply to MIFT.

To enable this capability, the Customer must complete the Global Manual Transaction Authorization (GMTA) form, which supplements the Master Account and Service Terms (MAST), and any other applicable account terms and conditions. The GMTA form must be signed by authorized signatories as listed in the Customer's Board Resolution or equivalent.

The GMTA form identifies those individuals who are authorized to initiate and confirm instructions by manual means, on behalf of the Customer.

Customers who do not provide a GMTA form to the Bank, and therefore do not have MIFT payment capability, understand that manual means of communication will not be available to them in the event they are required for contingency or other applicable scenarios that may involve manual instructions.

If a GMTA form is not presented by the Customer, the Bank accepts only the official PFNY11 transfer order form in original copy. (PFNY11 form can be used only for Hungarian ACH transactions.)

Notes for Completing the GMTA Form

1. The manual instruction can be sent to Citi via either one of the following communication modes. Please select the option(s) you want to activate in the GMTA form:
   - Letter
   - Fax

   Please contact your Citi representative for additional details.
2. Citi recommends that the nominees be located in the same time zone as the country where the Customer's Account is located.
3. When completing the GMTA form, the Customer should list all account numbers that are to be enabled for manual processing on the GMTA Account Information Schedule.

Processing MIFT Instructions

In the event that the Customer requires the Bank to process a MIFT instruction:

1. The Customer sends a manual instruction, duly signed, to Citi via the selected communication mode. For movement of funds from the Customer's Account, Citi recommends using the standard manual payment form.
2. Upon receipt of the manual instruction, the Bank carries out its internal verification, including, but not limited to, reviewing for completeness of the required processing details and verifying the initiators' signature(s) against those provided in the GMTA form. The Customer should

take care when completing the standard form for manual payment as it may be rejected if it contains erasures or white-outs.

3. The Bank refuse to execute payment orders which are not signed in accordance with the GMTA available to the Bank and, in such cases, the Bank notify the Customer accordingly. The Bank shall not be held liable for the consequences of executing any false or fraudulent payment order if the false or fraudulent nature cannot be discovered by the Bank, exercising its reasonable care. Damages, losses and/or costs related thereto shall be borne solely by the Customer.

4. The Bank may conduct an additional control by calling back the nominees included in the GMTA form. Confirmation by telephone may be recorded by the Bank.

5. The Bank processes the manual instruction once the Bank determines that all the verifications are successful.

Updates to Authorizations

If information provided in the GMTA changes, the Customer must submit a new GMTA form which supersedes the previous form. Changes for which the Bank should be informed include, but are not limited to:

- Personnel changes
- Changes to a person's name (e.g., due to change in marital status)
- New telephone numbers (e.g., a new phone number, new area code, or new city code)
- New account number

Neither a GMTA form detailing just the updated alone, nor a letter or any other form of document will be accepted. This is necessary to assure the operational integrity of the manual communication process.

Deletions to Authorizations

The Customer must submit the name of nominee to be removed from the GMTA form in a letter on company letterhead and signed by authorized signatories as per the Customer's Board Resolution or equivalent. Again, in the interest of operational integrity, the Bank will request a new GMTA form that will supersede all previous GMTA forms if there are several signature deletions.

VI. TTS Consolidated Security Procedures

As referenced in the Communications section of the Master Account and Service Terms (or other applicable account terms and conditions) ("MAST") that has been entered into between the Customer and the Bank the following is a description of the security procedures ("Procedures") used by Citi Treasury and Trade Solutions in connection with the following Services or connectivity channels.

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM"), TreasuryVision®, and WorldLink®)
- Interactive Voice Response ("IVR")
- Email/fax with the Bank excluding Manually Initiated Funds Transfer (MIFT)
- CitiConnect®
- Other local electronic connectivity channels

Availability of the Services or connectivity channels will vary across local markets. These Procedures may be updated and advised to the Customer by electronic means or otherwise from time to time. Customer's continued use of any of the above noted services or connectivity channels after being advised of updated Procedures (which may include, but is not limited to, the posting of updated Procedures on CitiDirect BE in connection with the service or connectivity channel) shall constitute Customer's acceptance of such updated Procedures. These Procedures are to be read together with the MAST as such MAST may be amended from time to time. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the MAST.

A. Security Manager Roles and Responsibilities*

For the applications accessible in CitiDirect BE, the Bank requires two separate individuals to input and authorize instructions; therefore a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating our communication via the Internet. Any such Communications, when authorized by two Security Managers, will be accepted and acted on by the Bank. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate its Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the bank) granting the Customer access to its Account(s). This only applies in relation to Account(s) covered under the relevant authorization.

*Security Manager Roles and Responsibilities may be prohibited in certain local market. Please contact your Customer Service representative for further information

The Security Manager function includes, but is not limited to:

1. Establishing and maintaining the access and entitlements of users (including the Security Managers themselves), including activities such as:

(a) creating, deleting or modifying User Profiles (including Security Manager Profiles) and entitlement rights (please note that user name must align with supporting identification documents)

(b) building access profiles that define the functions and data available to various users, and

(c) enabling and disabling user log-on credentials

2. Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same

3. Modifying payment authorization flows

4. Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users

5. Notifying the Bank if there is any reason to suspect that security has been compromised.

Security Managers also assign transaction limits to users for those Bank products to which the Customer has access. These limits are not monitored or validated by the Bank; Customer should monitor these limits to ensure in compliance with Customer's internal policies and requirements, including but not limited to, those established by Customer's Board of Directors or equivalent.

Specifically related to the **eBAM Application,** the following roles are required:

The initial set-up on the eBAM Service requires the designation of three Security Officers and one Corporate Secretary. Two separate Senior Administrative Roles act in concert as maker/checker to set up and assign User function/data entitlements and Workflows. These arrangements are not monitored or validated by Bank; Workflows and User activity are monitored by the Customer to ensure compliance with Customer's (and Account Owners') internal policies, requirements, and authorization and approval levels, including but not limited to those established by the Customer's (and Account Owners') Board of Directors or equivalent governing body.

The following roles are required for the eBAM Service:

1. **Security Officer:** fulfills functions described in (1) a-c above within the roles of Security Managers

2. **Corporate Secretary:** ensures that Workflows, Users set up as Designated Authorizers, and their assignment to Workflows meet internal policies, requirements, authorization and approval levels, as established by the Customer's (and Account Owners') Board of Directors or equivalent governing authority

3. **Designated Authorizer:** have broad, senior authority to initiate and authorize Workflow activities

4. **Request Initiators:** are individuals authorized to perform administrative activities such as entering account and signer management requests into the eBAM system

The Security Officers, Corporate Secretary, and Designated Authorizers are responsible for:

a) Defining and administering hierarchy setup and site/flow control, such as establishing Workflows and identifying Users and levels of approval

b) Creating additional Senior Administrative Roles and appointing Users thereto (who may or may not be employed by the Customer)

c) Notifying Bank if there is any reason to suspect that security or confidentiality of any User (including Senior Administrative Roles) credentials has been breached or compromised

d) Where relevant, completing, amending, approving and/or supplementing such Customer implementation forms as may be reasonably requested by Bank from time to time in connection with the provision of services and/or products to Customer

B. Authentication Methods

The Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users typically through mechanisms such as User ID / password pairs, digital certificates, and security tokens (deployed via hardware or software) which generate a dynamic password used to access the services or connectivity channels each time the Customer or a user logs in or authenticates themselves. Please note that availability of the Authentication Methods described below varies based on local markets.

Security Managers and all users who want to (a) initiate or approve transactions (and whose User Profile permits them to do so) and/or (b) access the systems in accordance with entitlements must use the available Authentication Methods (which may be updated from time to time as described above).

The following Authentication Methods are available to access the above-noted services or connectivity channels in combination with a User ID:

Authentication Method	***Description***
Token: Challenge Response	*Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a 4 digit pin. When accessing CitiDirect BE, the system generates a challenge, and a response passcode is generated by the utilized token and entered into the system.*
Token: One Time Password	*Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which is used to generate a dynamic password after authenticating with a 4 digit pin. This dynamic password is entered into the system to gain access.*
SMS One-Time-Code	*A dynamic password is delivered to a user via SMS, after which the user enters the dynamic password and a secure password to gain access to the system*
Voice One-Time-Code	*A dynamic password is delivered to a user via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system*
MultiFactor Authentication	*A dynamic password is generated via a SafeWord Card or MobilePASS token, after which such dynamic password is entered along with a secure password to gain access to the system.*
Digital Certificates	*A Digital Certificate issued by an approved certificate authority which is used for authentication. Digital Certificates utilize a Key Storage Mechanism and a*

	corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers.
Secure Password	*A user enters their secure password to access the system. A Secure Password typically limits a user's capabilities on the system, such that information can be viewed and no transaction capabilities are enabled.*
Interactive Voice Response ("IVR") & email	*Users contacting the bank will be prompted to enter a PIN number or provide other information to validate authorized access over the phone or over email.*
Fax	*Correspondence received by the Bank, excluding MIFT requests, will be signature verified based on the information that is contained in the Customer's board resolution.*
MTLS	*Mandatory Transport Layer Security (MTLS) creates a secure, private email connection between the bank and the external party. An email transmitted sent using this channel is sent over the Internet through an encrypted TLS tunnel created by the connection.*
Secure PDF	*Encrypted emails are delivered to a regular mailbox as a PDF Document that is opened by entering a private password, both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first Secure Email received.*

To learn more about any of these Authentication Methods, please refer to the Login Help page on CitiDirect BE (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

For CitiConnect®

- If the Customer chooses to use a public Internet connection to connect to Citi, including HTTPS, secure FTP, and FTPS, the Bank and the Customer will exchange security certificates to ensure both the communication channel and the messages exchanged are fully encrypted and protected. The Bank will only accept Communications originating from the Customer's secured communications gateway using the exchanged security certificates, and vice versa, and the Bank will only transmit Communications to the Customer's communication gateway using the exchanged security certificates.

- If the Customer chooses to use CitiConnect via SWIFT, then for any payment orders and instructions involving SWIFT, including amending or cancelling such orders, the Procedures that will be used to authenticate that a payment order or instruction is that of the Customer and authorized by the Customer shall be those as provided for in the SWIFT Contractual Documentation (as such term is defined by SWIFT and as may be amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in any other terms and conditions that may be established by SWIFT. The Bank is not responsible for any errors or delays in the SWIFT system. Communications to the Bank are to be provided in the format and type required and specified by SWIFT.

- If using a VPN, both the Customer and the Bank will designate a single IP address from which Communications between the Customer and Bank will be sent and/or received. The Bank will only accept Communications originating from the Customer's designated IP address, and vice versa, and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.

- The Customer and the Bank may also use a Hardware Security Module Authentication to accompany VPN Authentication. This requires the Bank and the Customer each to install a device on the servers designated for Communications between the Bank and the Customer.

The Bank requires:

- Customer's safeguarding of the Authentication Methods including any log-on credentials and/or security certificates associated with the Authentication Methods (collectively, the "Credentials") and ensuring that access to and distribution of the Credentials are limited only to authorized persons of the Customer. The Authentication Methods and associated Credentials are the methods by which the Bank verifies the origin of Communications issued by the Customer to the Bank.

- The Customer should take all reasonable steps to protect the Credentials. Accordingly, the Bank strongly recommends that the Customer does not share the Credentials with any third party.

Certain jurisdictions may require individuals (and their corresponding credentials) to be identified as compliant with applicable AML legislation requirements before granting access to perform certain functions.

The Bank understands that the Customer may, in some cases, wish to share the Customer's Credentials with a third party entity or service provider (including without limitation any third party payroll provider) designated by the Customer to have access to the Customer's Credentials (such third party entity or service provider shall be referred to herein as an "Authorized Third Party") for the purpose of accessing and utilizing any of the banks electronic channels on the Customer's behalf. In the event that the Customer elects to share its Credentials with an Authorized Third Party, the Bank strongly recommends that the Customer takes, and ensure that any Authorized Third Party takes, all reasonable steps to protect the Credentials from being disclosed to any non-Authorized Third Party personnel. The Bank is authorized to act upon any Communication that it receives from an Authorized Third Party on behalf of the Customer in compliance with these Procedures.

C. Data Integrity and Secured Communications

- The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the Internet, email and/or fax, which are not necessarily secure communication and delivery systems. The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during transit.

- If the Customer suspects or becomes aware of, a technical failure or any improper access to or use of the Bank's services, connectivity channels or the Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's services or connectivity channels.

- If Customer utilizes file formatting, encryption software (whether provided by the Bank or a third party), to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with Citi, then the Customer will use such software solely for the purpose for which it has been installed.

VII. Conclusion

Thank you for choosing Citi Treasury and Trade Solutions (TTS) for your cash management needs. Please feel free to contact your Citi relationship manager with any additional questions that you have regarding TTS Services.

Treasury and Trade Solutions
citi.com/tts