Cash Management User Guide

Poland

Treasury and Trade Solutions

citi handlowy

Table of Contents

I. Introduction

Thank you for choosing Bank Handlowy w Warszawie S.A. (the Bank) Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this Cash Management User Guide for Bank Handlowy w Warszawie S.A. is to provide customers with a manual containing detailed information of services available to them.

This guide is to be read together with the Local Conditions document, Master Account Service Terms (MAST), Regulatory Disclosure, Declarations and Representations (RDDR), Confidentiality and Data Privacy Conditions (CDPC), the Table of Fees and Commissions and setup forms. This guide may be updated by the Bank at any time upon notification to the Customer.

II. Payment Services

A. Types of Payments Services offered by the Bank in Poland

- Book Transfers: Transfers of funds between the Bank accounts
- Domestic Funds Transfers: transfers processed via Krajowa Izba Rozliczeniową S.A. (“KIR” system) system and SORBNET (the system of National Bank of Poland that supports both high-value and low-value transfers) on another bank account in Poland
- Real-Time Gross Settlement (RTGS): a large-value funds transfer system based on continuous settlement of payments on a gross, individual order basis, provided by National Bank of Poland (SORBNET2)
- Single European Payments Area (SEPA): a EUR clearing mechanism for, high-volume payments, which includes both a mandate-based direct debit service and a credit transfer service
- Faster Payments (Express Elixir): real-time domestic electronic funds transfers used to deliver funds from the Bank account to another bank accounts via KIR system. The maximum amount per transaction is PLN 100 000.
- Direct Debit: a means of collecting monies owed by a payer, where the beneficiary generates the initiating transaction to be processed by the payer’s bank against the payer’s account. Direct debit, which is always subject to the payer’s authorization, is typically used for recurring payments, such utility bills, where the payment amounts vary from one payment to another.
- Cross Border Funds Transfers: allow Bank customers to make international transfers in a wide range of currencies as outgoing telegraphic transfers.

B. Sending a Payment

1. The Customer sends a payment instruction to the Bank, formatted to market standards and as outlined at the time the payment service was implemented, via:
    - Bank e-banking channels, which include CitiDirect BE® and CitiConnect®, or
    - A SWIFT interface, or
    - Manually Initiated Funds Transfer (MIFT)
2. The payment instruction is authorized by the Customer if:
    - in case of connectivity channels – transactions are executed by the Customer as indicated in TTS Consolidated Security Procedures and submitted to the Bank via connectivity channel identified therein,

- in case of MIFT – the instruction is signed by the authorized persons according to the specimen signature card. Instructions are considered received if delivered to a Bank location identified as a location which accepts MIFT instructions,
- in case of SWIFT instruction, the Customer entered the payment instruction in the SWIFT system, so that Bank could read its content.

The Bank may introduce security procedures with respect to each form in which the Customer gives instructions. The Bank may confirm over the telephone any instructions that result in debiting the Account with the persons indicated by the Customer.

The Bank may refuse to carry out the instructions if:

- confirmation cannot be obtained by telephone, or
- confirmation is not identical to the content of the instructions sent to Bank.

3. Bank forwards the instruction to the relevant payment system for further processing
4. The payment system forwards the instruction to the beneficiary bank based on the locally defined clearing cycle.
5. The beneficiary bank credits the beneficiary account.

C. Receiving Direct Debits (Customer as Payer)

The Bank, as the Customer's Paying Bank, supports incoming direct debits instructions received from other participating financial institutions. The Bank supports payments through domestic direct debit in PLN and SEPA direct debit (CORE and B2B schemes).

Direct Debit Mandate

The Customer consents to have its account debited by signing a direct debit mandate. Mandates must include a unique Customer ID, unique recipient ID and unique payment ID. Mandates must be given to the recipient or the Bank in writing or in another previously agreed form. SEPA direct debit mandates (under the CORE scheme) must be given to the recipient only, and under the B2B scheme must be given to both the Bank and the recipient.

The Customer may withdraw a local or SEPA B2B direct debit mandate at any time by submitting a request that includes the following:

- the Customer's account number, name and signature
- the recipient's name
- the recipient's unique ID
- the unique transaction ID determined by the legal relationship between the Customer and the recipient.

The Bank will discontinue the direct debit service within 3 business days of receipt of the withdrawal request.

The Customer may not withdraw its mandate to execute SEPA direct debits under the CORE scheme.

Local Direct Debit Payment Refunds

The Customer may submit, within 5 business days of the day on which its account is debited, an instruction to refund a payment transaction carried out under the direct debit service. Refund requests may be submitted in writing to the address provided on the Bank's website or via CitiDirect BE®.

Refund requests should contain the following:

- the Customer's account number
- the recipient's unique ID
- the unique transaction ID determined by the legal relationship between the Customer and the recipient.
- the amount debited from the Customer account
- the day on which the Customer account was debited.

If the Customer uses SEPA direct debit service under the CORE scheme, it may submit a refund request within eight weeks of the day on which its account was debited. The refund request may only be filed in writing. The Customer may not submit a refund request for SEPA direct debit transaction under the B2B scheme.

Local Direct Debit Payment Cancellations

The Customer may submit a request to cancel a direct debit service payment transaction no later than the end of the business day preceding the agreed date on which the Customer account is to be debited. Such requests may be submitted in writing to the address provided on the Bank's website or via CitiDirect BE®.

Cancellation requests should contain the following:

- the account number and the unique recipient ID
- the unique transaction ID determined by the legal relationship between the Customer and the recipient
- the date on which the Customer account is to be debited.

The Customer may not submit a request for cancellation under SEPA B2B or CORE schemes.

Local Direct Debit Payment Refusal

The Bank may refuse to execute an instruction to debit the Customer's payer account under the direct debit service in the following situations:

- the funds in the Customer account are not sufficient to cover the full amount of the direct debit transaction
- the Customer account is closed
- no mandate has been issued for the direct debit

- the mandate has been withdrawn
- the data provided in the direct debit mandate does not match the data provided in the payment instruction initiated by the recipient
- a cancellation payment request has been submitted.

Direct Debit Process

1. The Bank compares the transaction received against the Customer's direct debit mandate before payments are made.
2. If the direct debit payment is in compliance with the Customer's direct debit mandate, the Bank processes the instruction and debits the Customer's account.
3. If there are insufficient funds in the Customer's account, the Bank will not process the direct debit payment and will send the unsuccessful debit status back to the direct debit payment system or partner bank.

The Bank will reverse any entry passed erroneously and debit or credit the relevant account.

D. Cash Withdrawals

The Bank offers cash withdrawals using a dedicated service provider as open cash withdrawals (cash counted in the Customer's presence at the counter) or closed cash withdrawals (cash packages in sealed secure envelopes and cash counted without the Customer's presence)

Open cash withdrawals can be made via:

- the Bank's branch, in local (coins and notes) or foreign currency (notes). A list of foreign currencies accepted by the Bank is available on the Bank's website. Customers may initiate this withdrawal in three ways:
  - presenting a signed check issued by the Bank
  - presenting withdrawal instructions signed by authorized persons

  These transactions are considered authorised, when presented at the Bank with appropriate signature.
  - sending a file via CitiDirect BE® according to the Bank's template structure (limit of PLN 5,000 or equivalent in a foreign currency per person applies). Such withdrawal requests can be executed only within a maximum three months from the initiation date

  These transactions are considered authorised, when executed by the Customer as indicated in TTS Consolidated Security Procedures and submitted to the Bank via CitiDirect BE.
- Post Office locations listed on Poczta Polska S.A.'s website (www.poczta-polska.pl), excluding locations marked as Postal Agencies; in PLN only.

Closed cash withdrawals can be made via cash counting units (CCU) in local (notes/coins) or foreign currency (notes only).

Post Office Withdrawals Process

1. The Customer completes a product setup form and designates the account that will be used for cash withdrawals
2. The Customer completes a cash withdrawal order, with a payment title formatted in accordance with the Bank's instructions, and sends it via CitiDirect BE®. These transactions are considered authorised, when executed by the Customer as indicated in TTS Consolidated Security Procedures and submitted to the Bank via CitiDirect BE.
3. For withdrawals exceeding PLN 30,000, the Customer sends an email on the following address:

   pze.wyciagibank@poczta-polska.pl and
   ekspres.pieniezny@citi.com

   by 12:00 p.m. at least four business days in advance. The email must indicate:

   a. withdrawal amount
   b. postal location, including the number and exact address
   c. name and surname of the remittee
   d. date of the cash withdrawal.
4. The Bank verifies the Customer account and funds are transferred. Withdrawal orders from any Customer account other than the one indicated in the product setup form are not processed. The withdrawal order is non-cancellable once the Customer's account has been debited.
5. On the business day following the funds transfer, the Customer will receive an email or text notification from the Post Office stating the funds are ready for withdrawal. Each notification will contain a transaction identification (UIP) number.
6. The withdrawal will be available within 7 business days of receipt of the UIP number in any selected post office location indicated on Poczta Polska S.A.'s website.
7. Collection of the cash withdrawal requires:

   a. presentation of the identity document the Customer indicated in the withdrawal order, and
   b. the UIP number. Lost UIP numbers can be obtained by contacting CitiService.
8. If the withdrawal cannot be made due to the lack of cash at a post office location, the Customer will be directed to the nearest location with sufficient funds.
9. If the cash withdrawal is not collected within seven days, the Post Office will transmit the unclaimed amounts to the Bank. The Bank will return the funds to the Customer's account no later than 12:00 p.m., four business days after receipt from the Post Office.

Closed Cash Withdrawals Process

1. The Customer sends a cash withdrawal order form (according to the template provided by the Bank) via the CitiDirect BE®, by 12:00 p.m. at least two business days prior to the desired withdrawal date. These transactions are considered authorised, when executed by the Customer as indicated in TTS Consolidated Security Procedures and submitted to the Bank via CitiDirect BE. If CitiDirect BE® is not operating, a cash withdrawal order may be sent by fax to 22 690 14 95 and the original must be delivered on the day cash withdrawal is made.
2. Coinage should be requested in multiples of 50 (rolls) or 500 (bags). The Bank will provide requested denominations on a best-efforts basis.
3. The Customer inspects the package and delivery confirmation slip. Damaged or improperly closed packages should not be accepted. If a package number does not match the delivery confirmation slip or if the delivery confirmation slip contains any corrections or deletions, the package should not be accepted. The Customer's signing of the delivery confirmation slip is tantamount to the package being found to be intact.
4. The sole proof of the value of withdrawal provided to the Customer is a bank statement.
5. The Customer opens and counts the contents of the package(s) in the presence of a minimum of two of the Customer's employees. If the amount indicated on the withdrawal order and the amount counted by the Customer do not match, the Customer must submit a complaint within two business days. Complaints must contain the original packaging, a copy of the collective specifications, coin roll packaging (if applicable) bearing the signature or the number of the person preparing the roll in question, and all other elements signed by the persons preparing them.
6. The locations of CCU may change at any time. The Bank will notify the Customer by letter or electronically and changes will apply to the Customer from the date specified in the notification.

Electronic Postal Transfer Process

1. The Customer submits a Cash Delivery Order via CitiDirect BE®. These transactions are considered authorised, when executed by the Customer as indicated in TTS Consolidated Security Procedures and submitted to the Bank via CitiDirect BE.
2. Requested funds, Poczta Polska S.A. commission and beneficiary details are transferred from the designated Customer account to Poczta Polska. The maximum amount of the order is PLN 99,999.99. Cash delivery is carried out by Poczta Polska S.A.
3. If Poczta Polska S.A. changes its commission, the Customer will be notified in writing. The changes apply to the Customer from the day specified in the notification.
4. If there are no funds available to pay the Poczta Polska S.A. commission, the Bank will withhold the execution of transfers that day and inform the Customer by phone. If no funds are available the following day, the Bank will return the funds to the Customer's account.

5. The cash will be delivered to the address indicated in the order within four business days of when the Customer submits the order. If the deliverer fails to find the beneficiary at the address, an employee of Poczta Polska S.A. will leave a notice and attempt to deliver the cash within the following seven days. When the second attempt of delivering cash proves unsuccessful, funds will be returned to the Customer's account indicated in the setup form and the Customer will be charged the commission for return.

III. Receivables Services

A. Receiving a Payment

1. The clearing system forwards the instruction to the Bank based on the locally defined clearing cycle.
2. The Bank credits the Account.

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

For SEPA credit transfers, the debtor bank must be in one of the 28 member states of the European Union, the four member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco or San Marino.

B. Direct Debits Collections (Customer as Recipient)

The Bank, as the Customer's receiving Bank, supports direct debit instructions received from the Customer to withdraw funds from a payer's bank account.

Upon the Bank's request, the Customer submits the mandate received from the payer. The mandate is the payer's consent to debit their account with the direct debit amounts based on their liabilities toward the Customer. The mandate is given to the Customer or the payer's bank in writing or in another form agreed with the payer's bank or with the Customer. Mandates must include three minimum components: a unique payer ID, unique Customer ID and unique payment ID.

Direct Debit Collection Process

1. The Customer ensures that payers have direct debit mandates in place before initiating a direct debit to the Bank.
2. The Bank executes direct debit instructions on the day indicated by the Customer in the instruction as the payment date:
    a. instructions must be received before 2:30 p.m. at least one business day in advance to be executed on the indicated date.
    b. if an instruction is submitted after 2:30 p.m. on the business day prior to the indicated date, the instruction will be executed on the business day following the indicated payment date.
    c. if the indicated payment date is the same day on which the instruction is submitted or a past date and the instruction is received before 2:30 p.m., the instruction is executed by the Bank on the next business day. If the instruction is submitted after 2:30 p.m., it will be executed on the second business day following its submission.
    d. if the payment date is not a business day, instructions will be executed by the Bank on the next business day.

3. The Customer may cancel direct debit instructions that have already been submitted to the Bank no later than two business days before the payment date indicated in the direct debit instruction, by 10:00 a.m.
4. The Customer's account will be credited with the amount of the direct debit on the next business day following the receipt of funds from the payer's bank.
5. Reports containing successfully completed direct debits are sent to the Customer. Specifications for the format and delivery of these reports are outlined in the Product setup form.
6. The Customer notifies the Bank of any discrepancies between the report and the account statement within 14 days of receiving the report.
7. The payer's bank may refuse to execute the direct debit instruction that it has received for any of the following reasons:
    a. the payer has not given a mandate to their bank or has blocked direct debit usage
    b. the payer has withdrawn a mandate previously given to their bank, in an effective manner
    c. funds available in the payer's bank account are not sufficient to cover the direct debit or have been attached by bodies authorised to do so;
    d. the payer's account has been closed
    e. the payer has submitted an instruction to their bank to cancel a direct debit that has not yet been executed
    f. the payer's bank does not offer direct debit settlements to its clients.

If the payer has requested the return of the executed direct debit (within the time limit provided by law or interbanking agreement concerning the use of direct debit) or if the direct debit mandate was not given by the payer, the Bank will debit the Customer's account with the amount of the executed direct debit along with interest arising from the payer's bank account agreement (including calculation of this amount towards the overdraft granted by the Bank). The Bank may request that the Customer file a statement of submission to enforcement in accordance with Article 777 of the Civil Procedure Code.

For domestic direct debits, the debtor bank must be in Poland.

C. Over-the-Counter Collections

The Customer can deposit cheques and cash over-the-counter at any the Bank branch. A list of foreign currencies accepted by the Bank is available on the Bank's website.

D. Cash Collection Services

The Bank offers cash collection using a dedicated service provider as open cash deposits (cash counted in the Customer's presence) or closed cash deposits (cash in a sealed secure envelope and cash counted without the Customer's presence).

Open cash deposit can be made via:

- the Bank's branch, in local (coins and notes) or foreign (notes) currency. A list of foreign currencies accepted by the Bank is available on the Bank's website. Cash will be deposited immediately.
- specific Post Office locations listed on Poczta Polska S.A.'s website (www.poczta-polska.pl) excluding outlets marked as Postal Agencies, in PLN only, at least 15 days after the submission of a relevant product setup form. If a deposit is received before 2:00 p.m. on a business day it will be deposited on the same day. If it is received after 2:00 p.m. on a business day or on a non-business day, it will be deposited on the next business day.

Closed cash deposits can be made via:

- Automated Deposit Machine (ADM), in PLN (notes/coins) or foreign (notes only) currency accepted by the Bank. PINs, access cards to premises and keys enabling ADM use are provided by the Bank via courier service.
- Cash Counting Units (CCU), dedicated service provider locations, updated list of Counting Units provided at the request, in PLN (notes/coins) or foreign (notes only) currency accepted by the Bank, coins do not exceed 5% of the payment value, at least seven days after the submission of the relevant product setup form.
- Post Office cash collection (Deposits Plus), Poczta Polska specific locations, in PLN only, coins do not exceed 5% of the payment value, at least 10 days after the submission of the relevant product setup form.

Closed Cash Deposit Process

1. The transport of Cash Deposits can be provided on the basis of a separate agreement between the Customer and the Cash Transportation Provider. Cash deposit transactions are considered authorised, when delivered to CCU, Post Office employee or ADM.
2. The Customer electronically completes the Bank deposit slip (e-BDS) for each cash deposit stating the declared value of the cash deposit and the account to be credited. Software for producing e-BDSs is available free of charge on the Bank's website (http://www.citibank.pl/poland/corporate/english/cash-operations-deposits.htm). Prior to installing the software, the Customer will produce back-up copies of all programmes and databases on the computer equipment on which the software will be installed.

Packaging Requirements for Closed Cash Deposits

a. A single secure envelope contains notes of a value of no less than PLN 5,000. Notes of the same denomination are tied in bands of 100 or the entire deposit is banded so that the notes cannot move about. The band states the date of the deposit, the number of notes, the denomination and the conversion value. Notes that are excessively worn, damaged, or bear numbers and serial codes that are illegible will not be accepted by the Bank.

b. Coins are packaged in bags or rolls. Tags on the bags or rolls state the date of the deposit, the number of coins, the denomination and the conversion value. Coins that are excessively worn, damaged, corroded, or worn out will not be accepted.

c. Currencies are packaged separately.

d. Each package must be secured in a manner that prevents it from being opened without visible breach of the packaging.

e. Each package is marked with the Customer's name, the name of the Bank unit receiving the deposit, and the package identification number.

f. One copy of the e-BDS must be attached to each package and be visible without opening the package. The other copy of the e-BDS should be placed inside the package. The contents of the package should match the value and the specifications given on the e-BDS.

3. If the amount given in digits on the e-BDS differs from the amount written in words, the amount written in words is considered by the Bank as the official amount. In the event of discrepancies of any kind between the wording of the original and the copy of the BDS, the wording of the original is considered by the Bank as the official wording.
4. Worn out and damaged PLN notes and coins will be returned and a discrepancy report will be issued. The Bank will forward worn out or damaged notes and coins to the National Bank of Poland. Worn out and damaged notes and coins that are not replaced by the National Bank of Poland must be collected by Customer from a location specified by the Bank.
5. Worn out and damaged notes and coins in foreign currency will be refused and should be collected by the Customer promptly (no later than two weeks after notification).
6. Foreign currency coins may not be accepted. If accepted, the Bank may charge a handling fee of the value specified in the Bank Table of Fees and Commissions.
7. The Customer’s account is credited according to the method of collection:

Account Crediting Timelines			
ADM	**Cash Counting Unit (open on business days)**	**Cash Counting Unit (open 24 hours a day)**	**POST OFFICE (Deposits Plus)**
Counted Amounts			
Delivered by 8:00 a.m. on a business day: same day Delivered after 8:00 a.m.: next business day **Exception:** Deposits delivered to an ADM in Słupsk are credited the second business day	Delivered by 1:00 p.m. on a business day: same day Delivered after 1:00 p.m.: next business day following the day of delivery	Delivered by 1:00 p.m. on a business day: same day Delivered after 1:00 p.m.: next business day following the day of delivery.	Delivered by 7:00 a.m. on a business day: funds transferred to the account on the same day Delivered after 7:00 a.m.: funds transferred to the account on the following business day
Declared Amounts			
Delivered before 8:00 a.m. on a business day: booked the same day Delivered after 8:00 a.m. on any day: booked the next business day	Delivered before 2:00 p.m. on a business day: same day Delivered after 2:00 p.m. on a business day: by 12:00 p.m. the next business day following the day of its delivery	Delivered by 7:00 a.m. on a business day: by 12:00 p.m. on the day of delivery; Delivered after 7:00 a.m. but before 2:00 p.m. on a business day: day of delivery Delivered after 2:00 p.m.: by 12:00 p.m. the next business day following the delivery	

If the Bank changes the location of Cash Counting Units or ADMs, the Customer will be notified in advance by letter or e-mail.

Discrepancy Reports are prepared for all discrepancies greater than or equal to PLN 50 for cash deposits in PLN and for discrepancies of any value for cash deposits in foreign currencies. Discrepancy reports are delivered via CitiDirect BE® or e-mail to the address specified in the product setup form.

The Bank statements or copies of Discrepancy Reports (if counterfeit coins or notes are found or the declared value on the deposit slip does not match the actual value of the package) are the sole proof of a cash deposit and confirmation that a Customer's account has been credited.

If the account indicated in the bank deposit slip (eBDS/BDS) differs from the one provided on relevant product setup form, or when the account given in the Bank deposit slip is incorrect, the appropriate account in the respective currency will be credited in accordance with product setup form.

Secure Envelopes for Closed Cash Deposits

The Bank offers secure and disposable envelopes with high quality self-sealing tape made of plastic, preventing it from being opened without visible breach of the packaging. Packets of secure envelopes are sent upon Customer request by courier to an address in Poland.

Orders of 3000 envelopes or fewer placed by 3:30 p.m. on a business day will be sent by courier on the following business day. Orders of fewer than 3000 envelopes placed after 3:30 p.m. will be sent by courier two business days later.

Orders of more than 3,000 envelopes require longer completion time (no more than five business days). The Customer will receive an email confirmation indicating expected delivery date.

E. SpeedCollect

SpeedCollect allows the Customer to identify and reconcile a large number of its payers across different payment channels and bank networks.

SpeedCollect is based on virtual accounts, which are 26-digit account numbers compatible with NRB and IBAN standards, known to the Customer's payers and to which payments are made. A virtual account number consists of three successive elements: XX CCCC CCCC CCCC IIII IIII IIII.

- the X digits are a 2-digit control variable, calculated each time by the Customer using the NRB/IBAN algorithm on the basis of other digits.
- the C digits are assigned to the Customer by Bank during implementation. This is a fixed part, usually consisting of 12 digits.
- the I digits are called the Infocode. They are assigned each time by the Customer to identify individual payers (or other units, e.g., orders, invoices, shops etc.). The Infocode is presented in reports and usually consists of 12 digits.

The Bank accepts DFT/ACH, RTGS, and cross-border funds transfers, including SEPA, and cash deposits via SpeedCollect virtual accounts.

Pre-service Arrangements

The Customer contacts the Bank to request SpeedCollect and the Customer and the Bank agree on:

1. the fixed part of virtual account numbering, i.e., digits on the C part
2. the actual account number to which the SpeedCollect payments will be booked
3. the method of booking payments with or without consolidation
4. Reporting: the Bank provides the Customer with sample SpeedCollect reports from which the Customer chooses a preferred format or it agrees with the Bank on a non-standard format and timeframe.

Service Usage

1. The Customer generates the SpeedCollect virtual account number and passes it to the payer (e.g., prints the number on the invoice delivered to the payer).
2. The payer makes payments to the SpeedCollect virtual account.
3. The Bank receives the payment and looks up the appropriate actual account number, then:
    a. for payments not covered by consolidation, the Bank books each payment separately. The Infocode can be found on the bank statement and in the SpeedCollect report.
    b. for payments covered by consolidation, the Bank books payments as a collective amount. Such payments are shown in bulk on the bank statement (one bulk booking after each Elixir clearing session). There are no details of individual transactions on the statement or SpeedCollect report, so the Bank provides additional reports (i.e., DCH files) showing details. However, bulk booking is possible only for local incoming DFT/ACH transfers. Some transactions (such as foreign currency transactions, cash deposits or Express Elixir Split Payments) are excluded from consolidation and are booked separately.
2. The Bank delivers SpeedCollect reports, whose contents may be different from that of bank statements
3. The Bank also can send text messages to Polish mobile phone numbers. Such text messages are a non-standard form of a SpeedCollect report.
4. If the actual account indicated for SpeedCollect payments is closed and the Customers gives the Bankinstructions regarding the actual account (such as transfer redirection) those instructions only apply to the actual account and not to any SpeedCollect virtual accounts.

F. Account Receivables Matching Service (ARMS)

The Bank Accounts Receivable Matching Service (ARMS) is a solution that provides the Customer with tailor-made reporting.

In particular, ARMS can be used for reconciling incoming transactions with expected ones by combining a complete range of payments channels and methods with enriched transaction data, which allows standardized reporting and, ultimately, straight-through reconciliations.

Pre-service Arrangements

1. The Customer contacts the Bank to request ARMS, and the Customer and the Bank agree on:
    a. input data: Information that will be used for reconciliations. This is based on data available within the Bank (e.g., MT940 data) for static reconciliations or input data provided by the Customer (e.g., a daily open receivables database) that can be combined with MT940, for example, for dynamic reconciliations.

b. processing logic: How input data should be converted into output data, including business logic, triggers, conditions and frequency

c. output data: The final report that will delivered to the Customer, showing input data processed per the processing logic

d. connectivity: Channels that will be used for transmitting input and output data

e. implementation process, including solution testing

2. The customer may need to sign a non-disclosure agreement before implementation for the service can begin

Service Usage

1. In the case of dynamic reconciliations, the Customer prepares its input data and transmits it via the agreed channel to the Bank.
2. The Bank converts the input data into output data as per the agreed processing logic.
3. The Bank prepares the output data and transmits it via the agreed channel to the Customer.

IV. Other Considerations

1. The Customer will make its own assessment of the legal, regulatory, tax and accounting implications of the services.
2. 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.
3. The clearing of payments and receivables is governed by the rules set by the corresponding clearing system. Both the Bank and its customers must adhere to these clearing rules.
4. Business days are defined at Monday through Friday, excluding statutory holidays.
5. An operational day is a period of time when the Bank accepts and processes orders and instructions. No orders or instructions are accepted outside of operational days. Operational hours are defined period of time (according to communicated cut-off times at www.citihandlowy.pl/strefaklienta) within an operational day and may vary for different type of instructions and services.
6. All complete payment instructions and requests received by the Bank during operational hours will be processed on the same day on a best-efforts basis. If requested, payment instructions will be initiated on a specific date or at the end of a specific period.
7. If an account has insufficient funds, a payment will not be executed until the funds are available. After three business days from the date of the initial payment instruction, if funds have not been received the instruction will be rejected.
8. Complete instructions or requests (including tax or other budget payments) received after operational hours are considered received and processed the next operational day. Incomplete instructions and requests received by Bank during an operational day will be rejected.
9. The Customers are required to state the purpose of payments and funds transfers. Supporting documents must confirm the purpose of funds transfers and payments. Acceptance times are defined by operational hours.
10. More detailed information on cut-off times, maximum amounts, rates, charges and contact information is provided on the Bank's website at: www.citihandlowy.pl/strefaklienta. User manuals for CitiDirect BE® are available on www.citidirect.pl.
11. Before the expiry of the notice period, the Customer must deliver instructions to the Bank on how to dispose of funds accumulated in the Account. If the balance of the Customer's VAT account is positive as at the expiry date, the Bank will wait for the confirmation of the Head of the Tax Office's decision to dispose of funds. In the absence of such information, the Bank will maintain the VAT account as non-interest bearing until the Bank receives information on the decision of the Head of the Tax Office and its implementation. The Bank will not charge any fees or commissions for these Accounts

nor execute any payment instructions with regard to them. When the Bank receives the Head of the Tax Office's permission to transfer funds accumulated in the Customer's VAT account to its settlement account, the Bank will promptly execute such an instruction and transfer the Customer's funds from its settlement account to another account indicated by the Customer. After completing these instructions, the settlement and related VAT account will be immediately closed.

V. Electronic Forms

The Bank offers access to the electronic forms exchange platform for CitiDirect BE® users.

Electronic forms allow users to significantly reduce the amount of paper documentation exchanged with the Bank.

The Bank will provide electronic form services after the customer has completed the appropriate set up form. The customer authorizes specific representatives to authorize Electronic Forms.

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 the Bank's 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 & 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 onnection 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
Multi-Factor 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 the Bank, 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 the Bank, then the Customer will use such software solely for the purpose for which it has been installed.
- The Customer accepts that the Bank may suspend the access of the Users to the Services that require the use of the Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) in order to safeguard the Services and/or Credentials.

VII. Conclusion

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

Treasury and Trade Solutions

www.citihandlowy.pl

Version: Poland, September 2018

Bank Handlowy w Warszawie S.A. with its registered office in Warsaw at ul. Senatorska 16, 00-923 Warszawa, entered in the Register of Entrepreneurs of the National Court Register by the District Court for the capital city of Warsaw in Warsaw, 12th Commercial Department of the National Court Register, under KRS No. 000 000 1538, NIP 526-030-02-91;the share capital is PLN 522,638,400, fully paid-up.