

citi handlowy

# *read* CitiService News

July 2025 | edition No. 7

## Service Shortcuts

Contact with CitiService:

 tel.: 801 24 84 24; 22 690 19 81

# CitiDirect® Digital Onboarding - managing the list of authorized account users

We would like to remind you that CitiDirect Digital Onboarding supports our clients in opening additional accounts using the Universal Onboarding Form. Currently, in Phase 1, the bank partially completes the form using the data we already have, and sends it to you for completion and signature. At this stage, the process is already digital but still initiated by a bank representative. [Click here to see how you can open an incremental account in 3 easy steps >>](#)

In the target model (phase 2), CitiDirect Digital Onboarding will allow you to self-initiate additional account requests at your convenience. You will also be able to manage transaction banking products and update the list of individuals authorized to operate the account – all directly on our CitiDirect platform.

Importantly, thanks to the module in CitiDirect – Digital Signer Management (which we plan to expand later this year) – you will have direct access to information about individuals authorized to operate on the account (Signers) and the ability to submit online documentation to add, change, or remove them. The bank will verify the documents and automatically update the Central Database of Signers. Since the process relies on electronic document exchange, it is crucial that all changes are submitted in a strictly defined manner to ensure timely updates.

**NOTE:** to update the list of Signers, it is necessary to provide full details of authorized persons. To do this:

- use the [Universal Maintenance Form](#)
- provide all AML Act-required data indicated in the form
- indicate individual business e-mail addresses of authorized persons (with the company domain)

**IMPORTANT:** submitting only registration documents without the required data does not constitute the designation of a Signer for banking matters.

## Categories of people authorized to operate on the account – Signers:

**Corporate** – signers authorized per Board Resolutions, Powers of Attorney, Commercial Registers, or other similar authority documents to act on behalf of the Customer in opening, closing, and maintaining accounts.

**Operating** – signers authorized to credit, debit, or otherwise operate any account on behalf of the Customer for any service provided by bank, subject to any restrictions specified next to their name. Transactional signing authority is outlined in the Board Resolution or other similar authority documents, specifying who can transact on accounts and how.

**Initiators** – individuals authorized to initiate and confirm fund transfers by manual means (as well as amend, recall, or cancel previous instructions).

**Confirmers** – to ensure the security of funds, the Bank reserves the right to confirm over the phone instructions that result in debiting the account. For confirmation, the Bank will contact one of the authorized persons listed in this section.

## Standardization and Global Consistency

This digital onboarding process aligns with Citi's global approach, enabling us to deliver a globally consistent client experience. As part of this effort, we are adopting standardized documents across Citi that outline the terms and conditions of service provision, including: [the Master Account & Service Terms](#), [the Confidentiality and Data Privacy Terms](#), [the Security Procedures](#), and [the Country Addendum for Bank Handlowy w Warszawie S.A.](#) These will replace the current documentation, primarily the General Terms and Conditions of Co-operation with Clients, after you sign the [Universal Onboarding Form](#). Please note that this standardization of documentation will not alter your existing terms of service with Citi Handlowy but will ensure a consistent documentation structure across our entire Group.

We believe these enhancements will significantly improve your experience with Citi Handlowy, providing more efficient service.

# List of banks holding nostro accounts for Bank Handlowy w Warszawie S.A.

We would like to draw your attention to the update of the list of banks holding nostro accounts of Bank Handlowy w Warszawie S.A. The following bank has been removed:

DEUTDEFF DEUTSCHE BANK AG, FRANKFURT/MAIN

**IMPORTANT:** the only correspondent for payments in EUR is Citibank EUROPE PLC Dublin.

**PLEASE NOTE:** it is advised to send MT103 messages directly to CITIPLPX, and to provide the name of the correspondent bank in tag 53-54 of the SWIFT message.

| Currency | SWIFT BIC   | Name of the correspondent bank                  |
|----------|-------------|---|
| USD      | CITIUS33    | CITIBANK N.A., NEW YORK                         |
| EUR      | CITIE2X     | CITIBANK EUROPE PLC DUBLIN                      |
| GBP      | CITIGB2L    | CITIBANK N.A., LONDON                           |
| CHF      | CITIGB2L    | CITIBANK N.A., LONDON                           |
| SEK      | SWEDSESS    | SWEDBANK, STOCKHOLM                             |
| DKK      | NDEADKKK    | NORDEA BANK DANMARK A/S, COPENHAGEN             |
| NOK      | DNBANOKK    | DNB BANK ASA, OSLO                              |
| AUD      | CITIAU2X    | CITIBANK NA, SYDNEY                             |
| JPY      | CITIJPJT    | CITIBANK, N.A., TOKYO BRANCH, TOKYO             |
| CAD      | CITICATTBCH | CITIBANK, N.A., CANADIAN BRANCH, TORONTO        |
| CZK      | CITICZPX    | CITIBANK EUROPE PLC, ORGANIZACNI SLOZKA, PRAGUE |
| HUF      | CITIHUHX    | CITIBANK EUROPE PLC, HUNGARIAN BRANCH, BUDAPEST |
| ZAR      | CITIZAJX    | CITIBANK N.A. SOUTH AFRICA, JOHANNESBURG        |
| RON      | CITIROBU    | CITIBANK EUROPE PLC, ROMANIA BRANCH, BUCHAREST  |
| TRY      | CITITRIX    | CITIBANK A.S., ISTANBUL                         |
| CNY      | CITIHKHX    | CITIBANK N.A., HONG KONG BRANCH, HONGKONG       |
| BGN      | CITIBGSF    | CITIBANK EUROPE PLC, BULGARIA BRANCH            |
| KZT      | CITIKZKA    | JSC CITIBANK KAZAKHSTAN, ALMATY                 |
| PLN      | NBPLPLPW    | NARODOWY BANK POLSKI, WARSZAWA                  |
| ILS      | CITIILIT    | CITIBANK N.A. ISRAEL                            |

An updated list of correspondent banks available on [bank website >>](#)



# Migration to ISO 20022 and its impact on Citi Handlowy’s clients with respect to SORBNET (RTGS) payments

Work is underway to adapt the formats of interbank messages to the new templates in connection with the migration to the ISO 20022 standard. Below we present some important points that require your particular attention.

SORBNET payments are made using the SWIFT network, and migration to the ISO 20022 standard (i.e. MX messages) will take place on 8 September 2025, in accordance with the schedule of the National Bank of Poland. The following changes will come into force on this day.

- 1. A new interbank format is being introduced for the return of completed transfers (pacs.004). Therefore, a new code and transaction description regarding the return of a previously made transfer – **RETURNED ITEMS** – may appear in your statements/reports.

Examples:

| MT940  | CAMT.053  |
|--|---|
| :20:<br>:25:502001024<br>:28:/1<br>:60F:C250102PLN88,88<br>:61:2501020102CN44,44NTRF3428200470//3428200470<br>/CTC/918/RETURNED ITEMS<br>:86:/PT/FT/PY/DETALE 1                   DETALE 2<br>DETALE 3                   DETALE 4/OB<br>/PKOPPLPW/BO/PL94103015080000004200020001/<br>BO1/0200020X XXXX XXXXX<br>X/BO2/02. 00020XXXXXXX XX/XX/BO3/02-000 20XXXXXX,<br>XXXXXX | <Acct><br><Id><br><Othr><br><Id>502001024</Id><br>...<br><br><AcctSvcrRef>3428200470</AcctSvcrRef><br><BkTxCd><br><Domn><br><Cd>ACMT</Cd><br><Fmly><br><Cd>MCOP</Cd><br><SubFmlyCd>OTHR</SubFmlyCd><br></Fmly><br></Domn><br><Prtry><br><Cd>918+RETURNED ITEMS</Cd><br><Issr>CITI</Issr><br></Prtry><br></BkTxCd><br><NtryDtls><br><TxDtls><br><Refs> |

At this stage, it will apply only to outgoing SORBNET payments that are returned (i.e. incoming returns) and will be visible in all types of statements. Outgoing returns (i.e. returns of incoming payments to your account) remain unchanged for the time being.

Implementation date: September 2025

- 2. You will continue to be able to use the MT101 *Request for transfer* service in its current form. For both regular payments and VAT Split Payment, the obligation to provide data in a structured form will remain in place. If, however you decide to start using the new MX messages for VAT Split Payment now, please – exceptionally, until further notice – use the pacs.008 message with the following instructions:

In the *Regulatory Reporting* field, enter the value “VAT53”

<pacs:RgltryRptg>  
  <pacs:Dtls>  
    <pacs:Inf>VAT53</pacs:Inf>  
  </pacs:Dtls>  
</pacs:RgltryRptg>

In the *Remittance information* field, as before, the information accompanying the VAT Split Payment transfer must be formatted correctly as follows:

/VAT/10n,2n/IDC/14x/INV/35x/TXT/33x

where:

- n – digits only (0-9);
- x – any character allowed by SWIFT

- 3. In the case of orders received via pacs.008 payment messages, the rule for determining the payment channel based on transfer amount will remain unchanged. Payments above PLN 1 million will be sent through the SORBNET system, while payments below PLN 1 million will be sent via the Elixir system, in accordance with the National Bank of Poland’s guidelines. To make a payment, each of the following MX message fields must be completed:

<Dbtr> ABC PLC  
<DbtrAcct> 51103015080000000xxxxxxx

Implementation date: September 2025

- 4. As part of the migration to the ISO 20022 standard, it is planned to change the requirements for address fields (e.g. recipient address). An unstructured address format (data entered as a single string) will be withdrawn and replaced with a structured address format (where each component has a specific label).

For SORBNET payments, both structured and unstructured address formats will be accepted during the transition period. It will not be possible to use a so-called hybrid, i.e. combining structured and unstructured address elements in one message.

Example of a Structured Address:

<Cdtr>  
  <Nm>John Smith</Nm>  
  <PstlAdr>  
    <StrtNm>Hoogstraat</StrtNm>  
    <BldgNb>6</BldgNb>  
    <BldgNm>Premium Tower</BldgNm>  
    <Flr>18</Flr>  
    <PstlCd>1000</PstlCd>  
    <TwnNm>Brussels</TwnNm>  
    <Ctry>BE</Ctry>  
  </PstlAdr>  
</Cdtr>

Example of an Unstructured Address:

<Cdtr>  
  <Nm>John Smith</Nm>  
  <PstlAdr>  
    <AdrLine>HOOGSTRAAT 6, PREMIUM</AdrLine>  
    <AdrLine>TOWER, 18TH FLOOR</AdrLine>  
    <AdrLine>1000 BRUSSELS, BELGIUM</AdrLine>  
  </PstlAdr>  
</Cdtr>

Transition period: September 2025 – November 2026 (structured or unstructured address accepted)

Implementation date: November 2026 (only structured address accepted)

- 5. The new MX messages allow for more fields and characters than the MT formats. Rich data from MX messages will be converted to the MT-specific format and included in your statements (such as MT940, MT942, MT950, etc.) for the time being. Therefore, as a result, it may be necessary to truncate the data if the content of an MX message exceeds the character limits supported in MT reports/extracts.

- 6. In the case of using pacs.009 payment message, please follow the SORBNET rules.

In the Local instrument/ Proprietary filed only following values are allowed:

DEPOZYT  
KREDYT  
LOKATA  
ODSILENIE  
PROCC  
REZERWA  
ZASILENIE

Example:

<LclInstrm>  
  <Cd>  
    <Prtry>wartości w nawiasach

If not allowed word will be used the payment will be rejected.

- 7. To process SORBNET payment correctly, using pacs.008 or pacs.009 message in fields Intermediary Agent 1;Intermediary Agent 2 ; Intermediary Agent 3 you must enter the unique bank identifier – **BIC** code. Otherwise (e.g. if name and address are entered) it may result in incorrect payment and/or delays.

Example:

<IntrmyAgt1>  
  <FinInstnId>  
    <BIC> BIC  
  
<IntrmyAgt2>  
  <FinInstnId>  
    <BIC> BIC  
  
<IntrmyAgt3>  
  <FinInstnId>  
    <BIC> BIC

- 8. Incoming SORBNET payments will be booked according to the instruction received from the ordering bank – including when a foreign currency account is indicated for crediting.

Implementation date: September 2025

Points 2-7 above apply to SORBNET payments initiated by you using SWIFT messages.

The bank is also working on implementing the ISO 20022 format for all payments and will inform you about any changes in advance. Up-to-date information can be found on [our website >>](#)

Additionally, please find general ISO-related information on global Citi website:

<https://www.citibank.com/tts/sa/iso-20022-migration/index.html>

# Cybersecurity and rules for safe use of CitiDirect



Irrespective of the multi-level security scheme implemented by the bank, users should always be aware of threats on the Internet. We remind you of the rules for safe use of the CitiDirect below.

## CitiDirect system login address:

- Enter the address of the CitiDirect login page manually in your web browser's address bar, or add it to your "Bookmarks" ("Favourites"). Never search for the login page using a web browser's search engine.
- Before you start logging in, make sure you are on the correct, secure page of the portal. Your browser must show a locked padlock in the address bar, which means that the connection is encrypted. The site address must start with "https."

## Login:

- Use the modern CitiDirect Mobile Token, which is assigned to a specific device, has strong verification protocols, time-based control mechanisms, and built-in security parameters. Combined with CitiDirect biometric authentication (fingerprints or facial recognition), it is a convenient and secure way to log in to CitiDirect.
- Check how to enable Mobile Token for the users: CitiDirect® Mobile Token [Enablement Guide for Security Managers](#). Then the users can easily activate their Mobile Token: [Mobile Token activation video >>](#) and log into [CitiDirect: Login video >>](#)

## Access and entitlements in CitiDirect:

- The Security Manager can manage user profiles, their permissions, and authentication tools (Mobile Token), as well as temporarily blocks selected users in the system (e.g. for security purposes). This ensures the security of funds and transactions.
- To appoint a Security Manager, please submit Channels onboarding [form >>](#)

## Intelligent Payment review:

Citi® Payment Outlier Detection (CPOD) – a sophisticated analytics tool that helps identify transactions that stand out significantly from past trends:

- Sophisticated analytics tool comparing current payments against historical payments.
- Helps identify materially different transactions compared to past trends.
- Powered by advanced machine learning algorithms that continually evolve and recalibrate.
- Outliers are flagged for review and approval or rejection by nominated users before payment is processed.

Citi Payment Outlier Detection is available through CitiDirect without any technological changes to the client's systems. To start using the tool, contact your Relationship Manager.

[More information about CPOD>>](#)

## Beware of malware sent via email:

- Recipients' mails verify e-mails based on the address of sender. Please note that in the case of CitiDirect system e-mails it is always [citidirectbe.notifications@citi.com](mailto:citidirectbe.notifications@citi.com), and in the case of CitiManager it is [citicommercialcards.admin@citi.com](mailto:citicommercialcards.admin@citi.com). The e-mails from Citi Handlowy will always come from domain [@citi.com](mailto:@citi.com).
- Citi Handlowy uses SPF, DKIM, and DMARC e-mail authentication mechanisms to enhance e-mail security and prevent spoofing and phishing attacks. If your company's mail server is set to recognize such certificates, the malicious e-mail would either be blocked from delivery or sent to the spam folder.
- Attention on attachments: our statements are encrypted, and notifications such as balances will always have masked details.

To learn more about some common scams, as well as cybersecurity best practices, visit [Bank Handlowy w Warszawie S.A. | Citidirect – Security \(citibank.pl\)](#) or sign up for a free "Online Safety" training [Online trainings | Bank Handlowy w Warszawie S.A. \(citibank.pl\)](#)






# 3 layers of anti-fraud protection

## - protect, detect, respond

There are three key steps to developing a strategic defense for your organization. The first step is to ensure that your organization is **protected**; the second is to ensure that if fraud or an attempted cyberattack occurs, your organization can quickly **detect** it; and the third step is to ensure that your organization has a plan to **respond quickly** and appropriately in the event of fraud or a cyberattack.

When developing a strategic defense, it is essential to consider three aspects of your organization in each of the above phases: **people, processes, and technology**.

|  | PEOPLE   | PROCESSES   | TECHNOLOGY   |
|--|--|---|--|
| <div><br/>PROTECT</div> | <ul style="list-style-type: none"><li>Educate employees</li><li>Set maker/checker controls</li></ul>   | <ul style="list-style-type: none"><li>Grant only the necessary access, review it on an ongoing basis</li><li>Remove unnecessary permissions from employees</li><li>Have a plan for high-risk scenarios</li></ul>  | <ul style="list-style-type: none"><li>Avoid using free accounts for business correspondence</li><li>Limit employee access to private email accounts and social media sites</li></ul>   |
| <div><br/>DETECT</div>  | <ul style="list-style-type: none"><li>Pay attention to the so-called “red flags” (email form and style, sender’s address)</li><li>Pay special attention to cases reported during trips, on Friday afternoons, or just before official holidays/days off</li></ul>                  | <ul style="list-style-type: none"><li>Confirm by phone any transfer request to a new beneficiary</li><li>Do not call back new or temporary phone numbers</li><li>Make sure you are calling someone you know, avoid calling new or unknown people</li></ul>  | <ul style="list-style-type: none"><li>Regularly update your antivirus and antimalware systems</li><li>Install operating system and program updates as soon as possible</li><li>Use technology to flag emails as phishing attempts</li></ul>  |
| <div><br/>RESPOND</div> | <ul style="list-style-type: none"><li>Send a warning/alert to people who know what to do in case of such incidents</li><li>Don’t be afraid to use the word “fraud” or “problem”</li><li>Act quickly, every minute counts in the process of stopping and recovering funds</li></ul> | <ul style="list-style-type: none"><li>Create a process before you need it</li><li>Define roles and responsibilities</li><li>Determine who needs to be informed, what they need to see, and when</li><li>Carefully review transactions on other accounts to make sure there are no other suspicious operations</li></ul> | <ul style="list-style-type: none"><li>Keep all possible traces, including computers</li><li>Engage a security expert to verify how the incident occurred and to assess vulnerability to further attacks</li><li>Consider performing a vulnerability test against further attacks – engage your IT department to send fake “phishing” emails to employees</li></ul> |

Use the power of CitiDirect tools:

- appoint a CitiDirect Security Manager
- always use a two-person authorization scheme for transfers
- consider introducing amount limits or restrictions on working hours in the system

# Bank Holiday: July and August 2025

Please note the following days in **July and August 2025** when orders received will be processed on the following business day due to currency exchange holidays (i.e., public holidays in the respective countries).

| JULY |          |
|------|----------|
| 1    | CAD      |
| 4    | USD      |
| 7    | KZT      |
| 14   | UAH      |
| 15   | TRY, UAH |
| 21   | JPY      |

| AUGUST |          |
|--------|----------|
| 1      | CHF      |
| 4      | AUD, CAD |
| 11     | JPY      |
| 15     | RON, PLN |
| 20     | HUF      |
| 25     | GBP, UAH |