

read CitiService News

June 2022 | edition No. 6

Service Shortcuts:

Extract from the Table
of Fees and Commissions

[Check >>](#)

Foreign
Exchange Rates

[Check >>](#)

Market
Analyses

[Check >>](#)

Online trainings

[Check >>](#)

Client
Zone

[Check >>](#)

Newsletter
archive

[Check >>](#)

Contact with CitiService:

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



Security: Business Email Compromise (BEC)

Business Email Compromise (BEC) is a type of attack in which criminals send fraudulent e-mails or invoices with a payment request, usually impersonating a person known from previous business contacts, e.g. a contractor.

When it happens:

- Fridays or holiday seasons, e.g. Christmas
- By the end of the working day
- Popular absence seasons, e.g. summer or winter holidays, long weekends, bank holidays

How it happens:

- INVOICE
Fake supplier invoice with a new account number
- PAYEE CHANGE
Business contact requests for payments to be made to a **new account**
- EXECUTIVE
Payment request from an **internal senior manager**
- REAL ESTATE
Changes to a beneficiary account **during a property purchase or sale**

How to avoid threats:

Particular attention should be paid to the processes of handling transfers and document circulation in the company.

- We recommend using the **„callback”** method, i.e. calling back the contractor, who is indicated in writing, in the invoice or in an e-mail, using the contact details available within the company. The change of the counterparty's account should be supported by additional verification (e.g. confirmation by phone with the counterparty, cover letter signed by persons authorized by the counterparty, preferably with the use of an **electronic signature**). Modification based on received e-mail may result in loss of funds.
- **Electronic invoices** (PDF files, images, scans) should always be verified for correctness - in particular, a bank account. Any differences should be cleared with the contractor to avoid sending payments to criminals' accounts.
- **Regular daily verification of bank accounts, statements and account operations should be an ongoing practice for businesses.**
- We also propose using **Citi Payment Outlier Detection** intelligent payment verification - an advanced analytical tool that helps identify transactions that differ significantly from previous trends. Detailed information on the operation of Citi Payment Outlier Detection can be [found at >>](#)

In the event of any suspicions of fraud, we recommend urgent contact with the bank to minimize the risk of losing funds.

[BACK >>](#)

Join our online
trainings!
CitiDirect BE step by step

[Register now >>](#)

CitiDirect BE: easier contact with HelpDesk

To facilitate access to our specialists, we are integrating and improving telephone service as part of the Infoline of the Customer Service Department - CitiService and HelpDesk.

For technical support related to CitiDirect BE service, you can call the following numbers:

☎ **801 24 84 24 , (22) 690 19 81,**

☎ **801 343 978 , (22) 690 15 21.**

All of the above numbers have been redirected to the joint CitiService Infoline soon.

After selecting the language of the conversation and listening to the message about the GDPR, please select:

- „1” to connect to CitiService (verification remains unchanged),
- „2” to obtain **technical support for the CitiDirect BE system** (verification by entering the **last 10 digits of the company's account** - which is important - does not have to be the main account).

If you have an individual method of verification, it remains unchanged.

The change of verification rules came into force in May 2022. Thanks to this, the identification is faster and easier, and thus it shortens the waiting time for a connection with a HelpDesk specialist.

Feel free to contact the CitiService and HelpDesk teams - our advisers are ready to answer your questions and assist with all operational and technical issues.

[BACK >>](#)

Join our online
trainings!

CitiDirect BE step by step

[Register now >>](#)

Cross-border payments: the default cost option

Please be reminded that as of 10 November 2018 **SHA (Shared) is the default charging option for foreign payments for beneficiary banks located in the European Economic Area.** The change was implemented pursuant to the guidelines of the Payment Services Act implementing the PSD2 directive.

Consequently, as of 10 November 2018 the SHA (Shared) charging option is indicated on the CitiDirect BE system screen as the default option.

Please be reminded that the charging option indicates the party that will bear the transaction costs.

With reference to the information previously provided, we would like to point out that:

- a. individual forms of foreign payment orders created in the CitiDirect BE system
- b. foreign payment orders imported to CitiDirect BE
- c. foreign payment orders provided via Host to Host (CitiConnect system)

have the charging option previously selected by you. The bank cannot interfere with your payment orders, therefore if you have selected the OUR option, your payment will be provided for execution with this option. At the same time, if no charging option has been selected, the system will set the default option - SHA (Shared), as prescribed by the rules mentioned above.

Therefore, we kindly ask you to make sure that your selected charging option meets your expectations and to modify the payment instruction if necessary.

Importantly, different rules apply to SEPA payments.

Pursuant to the European SEPA rules, the only admissible fee payment option is SHA (Shared) option - therefore, the Select Cost Option field cannot be used in CitiDirect BE for this type of orders.

In order to effectively make a SEPA order in our CitiDirect BE system, you should choose the SEPA payment method and fill out a form in accordance with the user's manual [CitiDirect BE - Payments >>](#)

Making SEPA orders by means of the Foreign Transfer payment method may result in the bank's longer execution time due to the possibility of errors made by the user, which will require additional explanation. Therefore, **we recommend that you use the special SEPA form.**

These guidelines also refer to the import of payments from the financial and accounting systems to CitiDirect BE or CitiConnect. Given the fact that it is a system connection, we encourage you to contact our Technical Support Team whose consultants will explain to you how to properly set up your SEPA order import, so that there are no mistakes and extended order execution time.

[BACK >>](#)

Join our online
trainings!

CitiDirect BE step by step

[Register now >>](#)

Valid identity documents: important due to the amendment of the AML Act

With the change of the AML Act, we would like to remind you of the obligation to update the identity documents (ID) with the bank in the event that the validity period has expired or there has been a change for other reasons. Details below.

In connection with the amendment to the Act on anti-money laundering and terrorist financing of March 1, 2018 ("AML Act"), new obligations have been imposed on obliged institutions, including banks, starting from October 31, 2021. These obligations are related to the application of financial security measures in a situation where there has been a change to the previously determined customer data, including persons authorized to act on behalf of the customer or ultimate beneficiary owner. Please be reminded that, banks are required to identify the customer and verify its identity on the basis of identity documents on a constant basis. Citi Handlowy performs these activities in particular towards persons authorized to act on behalf of the customer, i.e. persons indicated in the signature specimen card or entitled to authorize payments in electronic banking, program administrators and corporate card holders. The obligations imposed by the amended AML Act require ensuring that customer data, including those from ID of persons authorized to act on behalf of the customer, is valid. We would like to draw your attention to this as **lack of current data may result in blocking the possibility of performing a transaction by a person whose data is not up-to-date**, and this may result in the delay or even suspension of your company's transaction.

[BACK >>](#)

Join our online
trainings!

CitiDirect BE step by step

[Register now >>](#)

Self-service: do not wait and designate CitiDirect BE Security Manager!

CitiDirect BE self-administration feature is one of the tools which enables you to manage a bank account on your own, without additional documents exchange and the need to contact the bank.

CitiDirect BE Security Manager is a function designated to a person in your company. CitiDirect BE Security Manager is able to manage users' profiles and their entitlements as well as authentication tools (token, MobilePASS) on his/her own, without the need to contact the bank and send additional documents.

In order to ensure adequate support, it is necessary to designate at least two CitiDirect BE Security Managers, the bank recommends designate three.

Entitlements of the CitiDirect BE Security Manager:

- Creates and deletes CitiDirect BE users
- Configuration and modification of user's entitlements
- Configure CitiDirect BE according to your own preferences
- Possibility to disable a user immediately, e.g. in the case of losing the SafeWord card
- Generates reports concerning users and its entitlements
- Managing authentication tools (token, MobilePASS)

Security Manager is allowed to manage the system without the need to fill in applications, wait for their execution and without the need to contact the bank.

Benefits for your Company resulting from having the CitiDirect BE Security Manager function:

- Saving time
- Security - changes are made by two users, after every change, authorisation is required
- Paperless operation
- Better control over operations in the CitiDirect BE
- Reduction of expenses: free confirmations of payments, entitlements reports, mt940 reports etc.

How to add and modify CitiDirect BE user entitlements:

One of the tasks processed by CitiDirect BE Security Manager is to add and modify user entitlements. In order to make it easier, we have created the templates of standard user access profiles. These are the entitlements (without accounts yet) that are selected most frequently, bundled in groups.

Please get familiar with the [manual >>](#) and check how you can manage CitiDirect BE user entitlements on your own, without additional documents exchange and the need to contact the bank.

Applications and materials:

You do not have a Security Manager to manage CitiDirect BE yourself ?

[Designate Security Manager >>](#)

[CitiDirect BE User Guide >>](#)

For more details, you can also contact a CitiService advisor.

[BACK >>](#)

Join our online
trainings!
CitiDirect BE step by step

[Register now >>](#)

Bank holidays: June and July 2022

Please note below the days in **June and July 2022** when orders received on that day will be effected on the following business day due to a currency exchange holiday (i.e. a public holiday in a given country).

JUNE	
1	RO
2	GB, IT
3	CN, GB, HK
6	AR, BE, CH, DE, DK, FR, HU, IE, IS, LU, NL, NO, SE
10	PT
13	AU, CY, GR, PT, RO, RU, UA
16	Boże Ciało, AT, DE, HR, PL, PT, ZA
17	IS
20	US
22	HR
23	EE, LU
24	EE, LT, SE
28	UA

JULY	
1	CA, HK
4	US
3	CN, GB, HK
5	CZ, SK
6	CZ, LT
8	AE
11	AE, TR
12	TR
14	FR
15	TR
18	JP
21	BE

[BACK >>](#)