

# read CitiService News

August 2022 | edition No. 8

Service Shortcuts:

Contact with CitiService:

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

# Security:

## 8 Tips on How to Stay Safe When Shopping Online

System Protected

Online shopping has gained widespread popularity in recent years. It is seen as a convenient way that saves time and effort and gives greater choice for people. Needless to say, this has caught the attention of cybercriminals who take advantage of the opportunity. Citi Handlowy advises how to stay safe when shopping online.

### 1. PROTECT YOUR COMPUTER AND PHONE

A good antivirus software with a firewall feature is critical for keeping your computer safe. Also, make sure you have the latest version of your antivirus software, operating system and web browsers.

### 2. CONDUCT RESEARCH

Shop at a trusted site rather than shopping with a search engine. If you use smaller merchants, check their credibility and rates on external websites. No or only few positive comments should be a warning. Pay attention whether the merchant provided its address and phone number.

### 3. CHECK IF YOUR CONNECTION IS SECURE

Check if the URL of the website begins with "https" instead of "http" and look for a padlock icon in the address bar, which indicates the site is more secure and makes it harder for a fraudster to view the information you type. You can click on the padlock icon in the address bar and a pop-up will appear, displaying security certificate information and other significant security details. Most modern browsers display a green lock to indicate a secure connection between your browser and the site you are visiting.

### 4. BE CAREFUL WHEN CLICKING ON LINKS IN EMAILS

Look for any typos, changed order of letters in words or combination of two letters that together look like other letter, e.g. "r"+"n" put next to each other look like "m". Do not open any attachment or link if you are not sure it is from trusted source. If you have any doubts of the site is legitimate, please check with the merchant before you click on the attachment or link.

### 5. CHECK AVAILABLE PAYMENT METHODS

Offering only one payment method by a merchant should raise your suspicion. Trusted online merchants offer a minimum of a few online payment methods. Once you finish your shopping, you are asked to select a payment method. If you choose to pay using the transactional platform of your bank, you will be taken to your bank's website and asked to log on into your account and authenticate to make the payment. Make sure you have been directed to your bank's real page.

### 6. UNUSUAL DELIVERY OPTIONS

If a merchant asks you to pay for the delivery yourself, it should raise your suspicion. Trusted online merchants arrange the delivery on their own and include the delivery cost in the final bill.

### 7. SAVE THE COPY OF YOUR ORDERS

It's always a good idea to keep documentation of your online purchases for any potential return.

### 8. ONCE YOU FINISHED YOUR SHOPPING, SIGN OUT

After your shopping is complete, sign out to prevent other persons from unauthorized access to your account or cards.

In case of any suspicious situations please report immediately to CitiService by calling:

**(22) 690 19 81** or **801 24 84 24** or by email to [citiservice.polska@citi.com](mailto:citiservice.polska@citi.com)

CitiService Advisors are available from Monday to Friday, from 8 am to 5 pm. After these hours please send an email to the following address: [alert.fraud@citi.com](mailto:alert.fraud@citi.com)

BACK >>

# Business Cards: the documentation change

We would like to kindly inform you that **the documentation for Business Cards has changed.**

The changes are aimed to adapt applications and forms to the new self-service modules introduced in the CitiManager platform (online application for the card OLA and online management of cards OLM). At the same time, we reduce the number of documents by integrating separate forms for Credit and Debit Cards in one document for Business Cards.

The scope of changes includes, among others:

- introducing the definition of the *Person authorized to act on behalf of the User* and the *Program Administrator* (in place of the current definition of the *Proxy*),
- introduction of the *Cards Program Administrators Form* (in place of the *VISA Business Card Program Proxies Card* and the *VISA Business Debit Cards Program Proxies Card*) and the **cessation of collecting specimen signatures** (specimen signatures are determined as part of opening a bank account),
- **removing the field with the address of residence** from the *Application for a Business Card* and ceasing to collect and update data in this regard,
- removing of the *Business Card Application* as an attachment to the *Agreement for the Issuance of Business Cards and the Processing of Operations made with their Use* (applications for a Business Card will be submitted via the CitiManager platform as standard).

**From 1 August 2022, please use the forms marked with the reference number [STANDARD 062022](#).**

Applications submitted on the old forms will be processed only until September 30, 2022. The exception is the Application for a VISA Business Debit Card for contracts concluded until April 30, 2021, which is valid under the reference number [CUSTOM 062022](#).

We would also like to inform you that the new documentation is available at [www.kartybiznes.pl](http://www.kartybiznes.pl) in the Program Administrator Zone.

If you have any questions, please contact the Corporate Cards Service tel: **+48 22 692 25 52** or e-mail: [karty.obsługa.klienta@citi.com](mailto:karty.obsługa.klienta@citi.com).

[BACK >>](#)

# Migration of SWIFT messages to ISO 20022 standard

We would like to inform you that, in accordance with the SWIFT guidelines, starting November 2022, the requirement for banks to accept payment messages (MT1XX, MT2XX) in a format compliant with the ISO 20022 standard (XML format), enters into force.

Citi Handlowy will be ready for this change at the time indicated.

At the same time, the bank is working on migrating all other SWIFT messages to the ISO 20022 standard in XML format. The ISO 20022 standard for all messages (sending + accepting) will become mandatory in 2025.

As SORBNET (Polish RTGS) payments are executed using SWIFT network, Citi Handlowy expects for this type of payment to be also migrated to XML format in 2025.

Until then, if SORBNET payments are received in XML format, Citi Handlowy will process them using the MTXXX format. The format for Elixir (ACH) payments remains unchanged for now.

[BACK >>](#)

# 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 >>](#)

# Electronic Banking: User Zone

## 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 >>](#)

# Bank holidays: August and September 2022

Please note below the days in **August and September 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 Poland).

AUGUST	
1	AU, CA, CH, IE, IS
5	HR
9	SG, ZA
11	JP
15	Assumption Day, AT, BE, CY, ES, FR, GR, HR, IT, LT, LU, PL, PT, RO, SL
24	UA
29	GB, SK
30	TR

SEPTEMBER	
1	SK
5	CA, US
12	CN
15	SK
19	JP
22	BG
23	JP
28	CZ
30	CA

[BACK >>](#)