www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

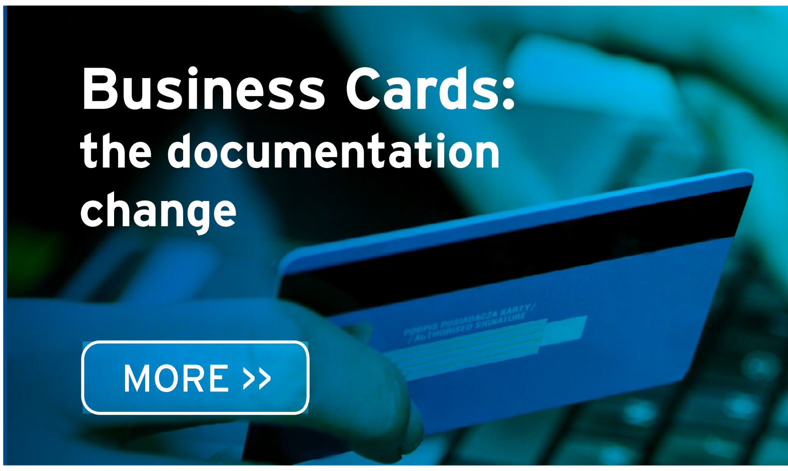
citi handlowy®

read CitiService News

July 2022 | edition No. 7

Security:
Ransomware

MORE >>

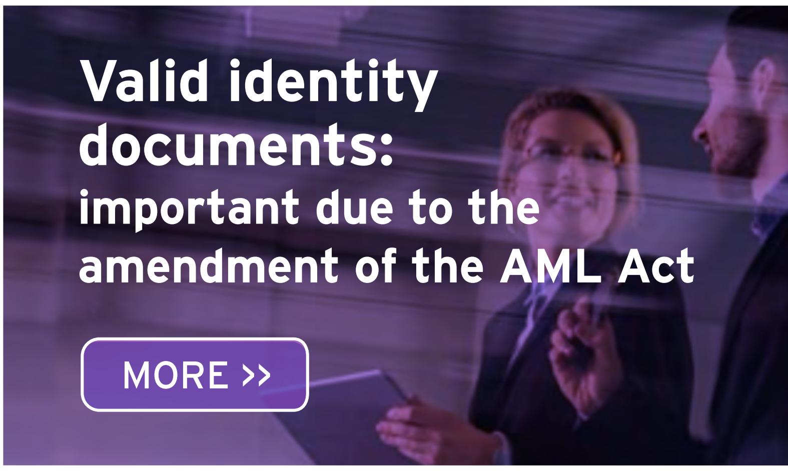


Business Cards:
the documentation change

MORE >>

Internal transfers:
processing changes

MORE >>

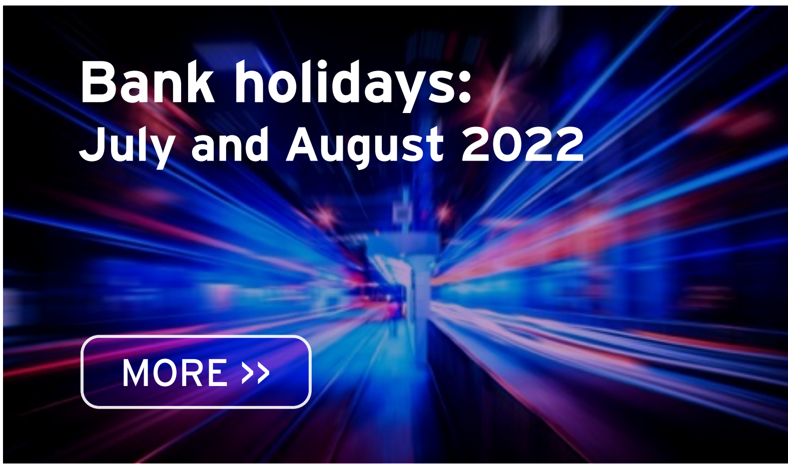


Valid identity documents:
important due to the amendment of the AML Act

MORE >>

Electronic Banking:
User Zone

MORE >>



Bank holidays:
July and August 2022

MORE >>

Service Shortcuts:

Extract from the Table of Fees and Commissions
Check >>

Foreign Exchange Rates
Check >>

Market Analyses
Check >>

Client Zone
Check >>

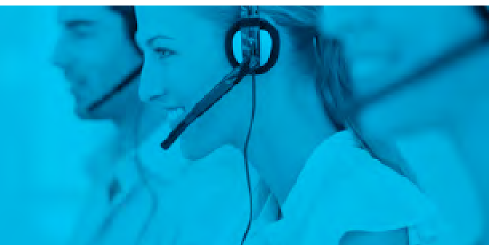
Newsletter archive
Check >>

Electronic Banking: Online trainings
Check >>

Electronic Banking: Video Instructions
Check >>

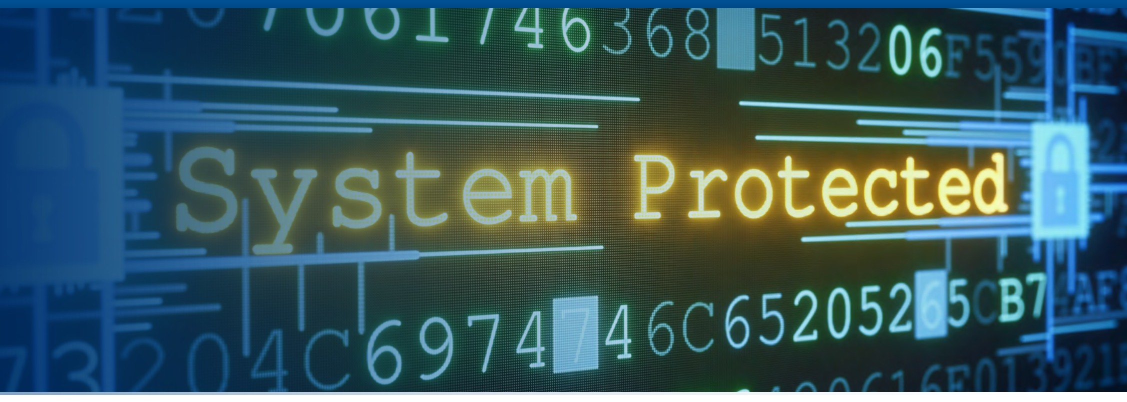
Electronic Banking: Manuals and documents
Check >>

Contact with CitiService:



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

Security:
Ransomware



Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files, demanding that a ransom is paid through certain online payment methods (and by an established deadline) in order to regain control of your data. It can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan). It is a scam designed to generate huge profits for organised criminal groups.

To prevent and minimize the effects of Ransomware, we recommend that you take the following actions:

- **UPDATE YOUR SOFTWARE REGULARLY**
  Many malware infections are the result of criminals exploiting bugs in software (web browsers, operating systems, common tools, etc.). Keeping these up to date can help to keep your devices and files safe.
- **USE ANTI-VIRUS SOFTWARE**
  Install and keep anti-virus and firewall software updated on your devices. Anti-virus can help keep your computer free of the most common malware. Always check downloaded files with anti-virus software.
- **BROWSE AND DOWNLOAD SOFTWARE ONLY FROM TRUSTED WEBSITES**
  Use official sources and reliable websites to keep your software patched with the latest security releases. Always use the official version of software.
- **REGULARLY BACK UP THE DATA STORED ON YOUR COMPUTER**
  Full data backups will save you a lot of time and money when restoring your computer. Even if you are affected by Ransomware, you will still be able to access your personal files (pictures, contact lists, etc.) from another computer. There are a number of high quality data backup solutions available on the internet for free.
- **CONSULT YOUR ANTI-VIRUS PROVIDER ON HOW TO UNLOCK AND REMOVE THE INFECTION FROM THE DEVICE**
  There are numerous official websites and blogs with instructions on how to safely remove this type of malware from your electronic devices. Always consult **www.nomoreransom.org** to check whether you have been infected with one of the Ransomware variants for which there are decryption tools available free of charge.
- **REPORT IT**
  If you are a victim of Ransomware, report it immediately to your local police and the payment processor involved. The more information you give to the authorities, the more effectively they can disrupt the criminal infrastructure.

REMEMBER:

- **DON'T CLICK ON ATTACHMENTS, BANNERS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN**
  What looks like a harmless advertisement or image can actually redirect you to the website from where the malicious software is downloaded. The same can happen when opening attachments in emails received from unknown sources.
- **DON'T INSTALL MOBILE APPS FROM UNKNOWN PROVIDERS/SOURCES**
  Always download from official and trusted resources only. In the settings of your Android device, always keep the option "Unknown sources" disabled and the "Verify Apps" option checked.
- **DON'T TAKE ANYTHING FOR GRANTED**
  If a website warns you about obsolete software, drivers or codecs (programs that encode and decode your data) installed on your computer, do not fully trust it. It is really easy for criminals to fake company and software logos. A quick web search can tell you if your software is really out of date.
- **DON'T INSTALL OR RUN NON-TRUSTED OR UNKNOWN SOFTWARE**
  Do not install programs or applications on your computer if you do not know where they come from. Some malware installs in background programs that try to steal your personal data.

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**

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**

BACK >>

Business Cards:
the documentation change

We would like to kindly inform you that **the documentation for Business Cards is changing**.

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 15 July 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** 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.obsluga.klienta@citi.com**.

BACK >>

Internal transfers:

processing changes

We are pleased to inform you that we have extended the hours of processing **internal transfers in PLN**. Payment orders that meet all of the following conditions:

- in PLN
- between corporate clients' accounts in Citi Handlowy
- on the domestic transfer form
- submitted **by 10:00 p.m.**

are carried out on the same business day.

NOTE: please pay special attention to the selection of the order form.

Different rules apply to payments requiring currency conversion. We remind you that orders between accounts in different currencies or the same foreign currency should be submitted on the foreign transfer form. The cut-off time for accepting orders on a foreign or SEPA transfer form between accounts in different currencies or the same foreign currency (even if both accounts are within Citi Handlowy) is 17:00. Orders placed after this cut-off time should have indicated the future value date (business day).

BACK >>

Designate Security Manager >>

to manage a bank account on your own, without additional documents exchange and the need to contact the bank.

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 >>

Designate Security Manager >>

to manage a bank account on your own, without additional documents exchange and the need to contact the bank.

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.

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.

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.

BACK >>

Designate Security Manager >>

to manage a bank account on your own, without additional documents exchange and the need to contact the bank.

Bank holidays:

July and August 2022

Please note below the days in **July and August 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).

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

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

BACK >>

This advertising material is for information purposes only and does not constitute an offer in the meaning of article 66 of the Civil Code. Links in our communication messages lead to websites or marketing materials of our Bank or our partners and are provided for information purposes. Links are not used to collect sensitive data from our Clients. In case of any doubts, please contact the sender of the message from the Bank. Citi and Citi Handlowy are registered trademarks of Citigroup Inc., used under license. Citigroup Inc. and its subsidiaries are also entitled to rights to certain other trademarks contained herein. 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 Division 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.