CIB BANK

Announcement

General Corporate Banking Business Regulations

for companies, other organisations and sole traders
Specific Business Regulations pertaining to Bank Cards

Specific Business Regulations pertaining to the CIB Mobilbank Electronic Service

effective from 1 July 2018

amendment

I. CIB Bank Zrt. (1027 Budapest, Medve u. 4-14.; company reg. no.: 01-10-041004) (hereinafter: Bank) hereby informs its Clients that with effect from 1 July 2018, the following sections of the Bank's General Corporate Banking Business Regulations shall be amended as follows (section 4.13 is a new provision).

2. Definitions

Beneficial Owner: the person defined as such in Section 3, 38 of Anti-Money Laundering Act.

4.4.1 The Bank shall, in accordance with the provisions of Anti-Money Laundering Act, perform a customer due diligence on (a check and identification procedure verifying the identity of) the Client, its Legal Representative, or the person with authority over the account, in the following cases:

a) when a business relationship is established with the Client, i.e. at the time that a written contract is concluded that relates to the Client, their authorised representative or the person that has access to their account;

b) when fulfilling a transaction order with an amount equal to or more than three million six hundred thousand forints;

c) when several transaction orders that are either known to be interrelated or that are suspected of being interrelated are given, at the time that the transaction order is given that results in the exceeding of the three million six hundred thousand forint threshold limit;

d) in the event that data, facts or circumstances indicative of money laundering or terrorism financing arise, if due diligence has not yet taken place as referred to above;

e) in the case of currency exchange transactions involving three hundred thousand forints or more; and

f) in all such cases in which there is doubt regarding the veracity or adequacy of the earlier recorded customer identification data or whether it is up-to-date.

4.2.1. In the course of the identity verification and identification process, the Client shall issue a written declaration to the Bank as to whether it is acting on their own behalf or in their own interest or on behalf or in the interest of the Beneficial Owner, and shall also declare to the Bank in person, in writing the data of the Beneficial Owner of a customer that is a legal entity or an organisation without a legal personality or the data of the Beneficial Owner prior to the conclusion of the Agreement in order to prevent any abuses related to the drafting of the Agreement and to the products and services, and in order to ensure compliance with the obligations stipulated by the Anti-Money Laundering Act. If during the contractual relationship doubt arises as to the identity of the Beneficial Owner, the Bank shall request the Client to make a repeat declaration.

4.2.2. The Bank may require from the client, other than the data specified in the Anti-Money Laundering Act, a declaration as to whether its Beneficial Owner is considered a politically exposed person. If the Beneficial Owner is a politically exposed person, the declaration must specify the section of the Anti-Money Laundering Act pursuant to which he/she is considered a politically exposed person.

4.3. Documents required for identification

In the course of the identification, the Client shall present to the Bank the following valid document(s) or a certified true copy/copies thereof (or – based on an agreement to this effect – the authentic electronic document(s) complying with Section 195, (1)-(4) and (8) of the Code of Civil Procedure), the validity of which the Bank must verify:

4.3.1. The following documents of the person(s) authorised to proceed in the Client's name or on its authorisation:

a) in the case of a natural person Hungarian citizen: an official document suitable for personal identification (personal identity card, passport or card-type driver's license – in the case of a minor, the birth certificate is also acceptable) and their official address certificate (or, in the case of a minor, an official certificate of the personal identification number);

b) a foreign natural person shall present his or her passport or personal identity card, provided that it authorises such person for residing in Hungary, or else a residence permit or a permit containing authorisation for residence;

c) The Bank shall make a copy of the document presented for the purpose of verifying personal identity; in the absence thereof no business relationship can be established.

d) the document proving the right of representation, if such right of representation cannot be established on the basis of the documents defined in Section 4.3.2;

4.4. In the course of the identification procedure, the Bank shall record the following data:

4.4.1. With respect to a natural person

a) family and given name

b) family name and first name (name at birth);

c) address or, in the absence thereof, place of residence;

d) place and date of birth;

e) nationality;

f) mother's maiden name;

g) type and number of identification document;

4.4.2. With respect to a legal person or an organisation without legal personality

a) name and the abbreviated name;

b) address of the registered office, and in the case of businesses with a registered office abroad – the address of their Hungarian branch, if any;

c) core activity;

d) in the case of a business organisation registered in the trade register, the company registration number, in the case of other entities, the number of the resolution on establishment (registration) or the registration number;

e) names and job titles of the authorised representatives;

f) data suitable for identifying the person authorised to receive consignments.

g) tax number

4.5. The presentation of a copy of the document required for identification shall be also acceptable if:

4.5.1 notary or a Hungarian representation abroad authenticated it in accordance with the rules of certifying the authentication of copies, pursuant to Act XLI of 1991 on Notaries Public; or

4.5.2. the copy has been prepared by an authority of the state of issue of the document duly authorised to prepare authentic copies, and – unless otherwise provided for by an international contract (including, in particular, Decree 11 of 1973 announcing the treaty issued on 5 October 1961 in the Hague on the abolishing of the requirement of any diplomatic or consular authentication (counter-authentication) in the case of public documents used abroad, during the effect of which an "apostil" is required, or any such bilateral international conventions pursuant to which a document authenticated by a foreign notary public may be used in Hungary without an apostil or counter-authentication, in accordance with its intended purpose) – the signature and stamp of such authority indicated on the copy has been counter-certified by a Hungarian consular officer, with the proviso that if an apostil is not stipulated by an international contract, the Bank may declare that it only accepts documents provided with an apostil.

4.8. Supplementary identification

The Bank – in the interest of compliance with the law (including, without limitation, the Anti-

Money Laundering Act and Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds), in accordance with its business policy applied in order to prevent money laundering and terrorism financing, and subject to the conditions defined therein – may refuse to execute certain (primarily payment) Transactions, or may request additional data in relation to the execution of such transaction orders, including especially, but not limited to, requests for data relating to the identification and actual activities of the Client, the Paying Party and persons and organisations within the Client's sphere of interest, and requesting that the underlying documents be presented. The Bank shall, subject to the Client's immediate written notification, refuse to execute the Transaction, or shall execute the Client's Transaction order for the crediting of the funds received from the Paying Party in accordance with the modified procedures (especially, but not limited to, late performance, or a price/rate appropriate for late performance), if the Client fails to provide data in response to the request for information, or if – in the Bank's opinion – it cannot be established from the provided data that the transaction order is in harmony with the data of the Client that is available to the Bank on the basis of the statutes.

4.13. After 26 June 2019 the Bank shall refuse to execute a transaction order if the Bank established a business relationship with the Client before 26 June 2017 and failed to perform the client due diligence measures by 26 June 2019, and the results of the client due diligence are not fully available with respect to the Client.

9.1. Unless otherwise provided by the Agreement, the Agreement may be terminated in writing:

9.1.1. the Client has the right to termination without explanation with 15 days' written notice (in the case of a [Framework] Agreement related to a Bank Account, a Payment Transaction, a card acceptance service or a Bank Card - free from fees, costs or other payment obligations in the case of a Framework Agreement existing longer than six months of a micro enterprise - with a notice period of 1 month, while in the case of a CIB Mobilbank Service with a notice period of 2 Banking Days);

9.1.2. The Bank may terminate, without explanation, with 30 days' written notice of termination (in the case of a (Framework) Agreement related to a Bank Card, Bank Account and Payment Transaction, an Agreement for card acceptance service, CIB Mobilebank and Electronic Service with a notice period of 2 months, and a safe service agreement with a notice period of 15 days), with the proviso that the Bank may not terminate an Agreement for a fixed-term Loan with ordinary termination.

14.4.3 c) In respect of unapproved payment transactions,

- that have been made with Sensitive Payment Data or with a Password Generator device or, in the case of the CIB mobilToken/CIB Bank mobile application, with the mobile device/mobile phone, that have been mislaid by the Card Holder or stolen, or that originate from unauthorised use of the Sensitive Payment Data or the Password Generator device or, in the case of the CIB mobilToken/CIB Bank mobile application, the mobile device, the Client who concludes an Agreement for such Internet-based Electronic Service, and/or

- that have been made with a Bank Card that has been mislaid by the Card Holder or stolen, or that originate from other unauthorised use of the Bank Card, the Client and/or

- that have been made with a T-PIN Code that has been mislaid by the Card Holder or stolen, or that originate from other unauthorised use of the T-PIN Code, the Client and/or

- that have been made with a password or codeword that has been mislaid by the Card Holder or stolen, or that originate from other unauthorised use of the password or codeword, the Client

shall bear the damages in an amount up to the equivalent of HUF 15,000 prior to the time of the Blocking.

The Bank is responsible for losses sustained after the blocking. in the case of the CIB Internet-based Electronic Service the Bank is liable up to a limit of HUF 15 million, with the proviso that this limit shall not be applicable to Clients that are classified as micro-enterprises under the prevailing regulations on payments.

If the object of the blocking mentioned above has been used without its physical presence or without its electronic identification, the Client defined above shall bear no liability, even up to the amount of HUF 15,000.

The Client shall bear no liability

- the paying party could not notice the theft, loss or unauthorised use of the cash-substitute payment instrument before the execution of the payment transaction,

- the damage was caused by a measure or omission of the Bank's employee, payment intermediary, or entity performing outsourced functions for the Bank,

- the damage was caused by a personalised process, which is the object of blocking, that took place using an information technology device or telecommunications device, or if such was used without the personal security elements – such as the PIN code or other Sensitive Payment Data.

- the Bank did not comply with its obligation to ensure the opportunity for the Client to make the Blocking any time.

The Bank shall be exempt from its above liability if it can prove that the loss incurred in connection with the unapproved payment transaction was caused by the fraudulent conduct on the part of the Client, or by the Client's wilful or grossly negligent breach of his/her obligations pertaining to the secret and secure storage of the device, the bank card or Sensitive Payment Data, or an obligation related to Blocking.

In the event of a Client report concerning an unapproved payment transaction, the Bank will examine each case individually, taking into account all the circumstances of

the case during the review, with regard to the fact that the use of a cash-substitute payment instrument does not in and of itself prove that

- the Client has acted in a fraudulent manner, or
- the Client has approved the payment transaction, or
- the Client wilfully or grossly violated his/her obligation to keep personal authentication data safe, or
- the Client has wilfully or grossly violated his/her obligation to report immediately after it comes to his/her attention the loss, theft or the unauthorised or unapproved use of a cash-substitute payment instrument.

Based on the above the Bank , by taking into account the outcome of the particular inquiry, shall consider the following cases wilful or gross negligence:

- if the Client records the Sensitive Payment Data in his/her phone, or on paper or another accessible place, or stores it together and in the same place with the device or the bank card (gross negligence);
- the Client transfers, makes available in any other manner or assigns to another person the device, the bank card or the Sensitive payment data or pledges them as security for a transaction or as a security deposit with a third party, or allows someone else to use it, or uses them for illegal purposes (especially, but not limited to, purchasing a product that is prohibited by the effective statutory regulations or purchasing prohibited services.) (gross negligence);
- possession or theft of the bank card by an unauthorised third party, if this has occurred as result of the Client's wilful misconduct or gross negligence, particularly as a result of the fact that the object used for storing the device/bank card or the device/bank card itself was left unattended, (wilfulness, gross negligence);
- failed, late or incomplete fulfilment of the obligations related to Blocking; (wilfulness, gross negligence);

The Bank shall not be liable for damages arising from blocking, even if such blocking was not executed by the Client (e.g. by the User or the Card Holder) (unauthorised reporting). The Bank shall be liable for any damage that originates from the fact that the Client was unable to make the Blocking due to reasons attributable to the Bank.

With regard to the time of the blocking request, the time recorded by the Bank shall be definitive until proven otherwise. Liability for keeping confidentiality/secure storage of any device, bank card or Sensitive Payment Data, as well as for any measures taken to this end shall lie with the Client.

II. The Bank hereby informs its Clients that as from 1 July 2018, the following sections of the Bank's Specific Business Regulations Pertaining to Bank Accounts of companies, other organisations and sole traders are amended as follows.

2. BANK CARD PIN CODE

2.1.The Card Holder shall act as generally expected under the given circumstances to keep the PIN Code safe, and thereby assume responsibility for ensuring that the Bank Card PIN code remains secret it cannot be accessed by another person. The Card Holder may not write down the Bank Card PIN Code or record it on the Bank Card or any other object that is kept together with the Bank Card.

2.2. The Card Holder is obliged to notify the Bank without delay by telephone (CIB24) if his/her Bank Card PIN Code has come to the knowledge of an unauthorised third party.

If the Bank Card PIN Code is lost or forgotten, the Client may request that the Bank Card PIN Code is resent, in writing, subject to fee payment as specified in the List of Conditions. In this case, the Bank shall send the Client the current PIN Code of the Bank Card. After the request for the resending of the Bank Card PIN Code has been received by the Bank, the PIN code associated with the Bank Card may be used until it is re-delivered to the Client.

If the Bank Card PIN Code has come into the possession of unauthorised persons, the Client may request blocking and replacement of the Bank Card in writing, in the case of replacement for the fee determined in the List of Conditions. If a request for the blocking and replacement of the Bank Card is submitted, the Bank shall send a new Bank Card PIN Code to the Client within 14 days following the request.

The Client may initiate the replacement of the Bank Card PIN Code, besides the case described above, in the case specified by the SBR applicable to CIB24 and orders placed via recorded telephone line, through a recorded telephone line, if the Client possesses a T-PIN. In this case a new Bank Card PIN Code is provided for the existing Bank Card. Replacement of the Bank Card PIN Code may only be requested for an activated Bank Card.

2.3. The Card Holder may change the Bank Card PIN Code to a four-digit number chosen at his own discretion, via an ATM operated by the Bank. The original PIN Code related to the Bank Card cannot be restored.

2.4 If the Client enters the wrong PIN Code at least three times, the Bank shall block the Bank Card. In this case, the Client may request, in the bank branch, via CIB24, or, in the case specified by the SBR applicable to CIB24 and orders placed via recorded telephone line, through a recorded telephone line, that the unsuccessful attempts be deleted if they have not forgotten the Bank Card PIN code or that the PIN code be replaced if they have forgotten the PIN code. Deletion of unsuccessful attempts takes place immediately for requests placed via CIB, while in the case of a request placed via a recorded telephone line, as described by the SBR applicable to CIB24 and orders that may be placed via a recorded telephone line, no later than 24:00 hours on the next Banking Day. After deletion of the unsuccessful attempts, the Bank Card may be used again with the existing PIN Code.

3.16 The Bank issues the Card Holder with a Bank Card PIN Code linked to the Bank Card, and hands it over to the Client/Card Holder in accordance with the provisions of section 1.10 of these Specific Business Regulations. With a knowledge of the Bank Card PIN Code, the Card Holder may perform Cash Withdrawals With a Bank Card from automatic teller machines (ATMs) displaying the appropriate logo, and at the Bank Branches, and may make purchases at electronic (POS) terminals that require the use of the Bank Card PIN Code. The Card Holder shall act as generally expected under the given circumstances to keep the Bank Card and the PIN Code safe. The Card Holder shall use the Bank Card and the PIN Code properly and lawfully.

5.4. In respect of unapproved payment transactions that have been made with a Bank Card that has been mislaid by the Card Holder or stolen, or that originate from other unauthorised use of the Bank Card, the Client shall bear the damages in an amount up to the equivalent of HUF 15,000 up to the time of the reporting of the Bank Card's having been mislaid by the Card Holder, its theft or unauthorised or unapproved use. The Customer shall not bear the liability referred to in this section if the Client or the Card Holder could not notice the theft, loss or unauthorised use of the cash-substitute payment instrument before the execution of the payment transaction, and also if the damage was caused by a measure or omission of the Bank's employee, payment intermediary, branch or entity performing outsourced activities for the Bank, or if the damage was caused with a personalised procedure classified as a cash-substitute payment instrument, which took place using an information technology device or telecommunications device, or if the cash-substitute payment instrument was used without the personal security elements – such as the PIN code or other code – or if the Bank breached its obligation to provide the Client with a 24-hour reporting opportunity. Following the reporting referred to in point 5.2 above, the Bank shall be liable for damages in respect of unapproved payment transactions made with a Bank Card that have been mislaid by the Client or stolen, or that originate from other unauthorised use of the Bank Card However, the Bank shall be exempt from its above compensation liability if it can prove that the damage generated in connection with the unapproved payment operation was caused by the Client's proceeding in a fraudulent manner, or if that the damage was caused by the Client's wilful or grossly negligent breach of his/her obligations pertaining to the use of the Bank Card as specified in section 3 or his/her reporting obligation mentioned above. With regard to the time of the blocking request, the time registered by the Bank shall be definitive. The Bank reserves the right to initiate legal proceedings against the Card Holder in the event of fraud related to the Bank Card that was committed by the Card Holder or by another person with the collusion of the Card Holder. The Bank is exempt from liability if having individually examined each circumstance of the case it proves that the damage originated from wilful or grossly negligent breach of contract on the part of the Client or the Card Holder.

III. The Bank hereby informs its Clients that as from 1 July 2018, the following sections of the Bank's Specific Business Regulations Pertaining to the CIB Mobilbank electronic service are amended as follows.

4. TERMINATION OF THE CIB MOBILBANK SERVICE

4.1 The Service may be cancelled by the Client at any time, without having to give a reason, with a 2 Banking Day notice.

4.2 The Bank shall have the right, based on a notice sent to the Client in advance, to cancel the Service at any time, subject to the observance of a 2-day notice period.

CIB Bank Zrt.

Date of publication (displaying): 29 June 2018