CIB BANK

Announcement

General Retail Banking Business Regulations

Specific Business Regulations pertaining to Bank Cards for Consumers

on the amendment of the Specific Business Regulations Pertaining to the CIB Internet-Based Electronic Services for Consumers and Sole Traders

with effect from 1 July 2018

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 Retail Banking Business Regulations shall be amended as follows (section 4.12 is a new provision).**

2. Definitions

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

4.1. The necessity of identification

The Bank shall, in accordance with the provisions of the Anti-Money Laundering Act, perform a check and identification procedure verifying the personal identity of the Client, the Client's Legal Representative or proxy, or the person with authority over the account, in the following cases:

4.1.1. 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, his authorised representative or the person that has authority over his account;

4.1.2. when fulfilling a transaction order the amount of which is equal to or more than three million six hundred thousand forints;

4.1.3. 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 will result in the exceeding of the three million six hundred thousand forint threshold limit;

4.1.4. 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;

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

4.1.6. 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.

4.2.2. The natural person Client shall issue a written declaration at the Bank, or using a secure, protected and pre-audited electronic communications device operated by the Bank, as to whether he/she is considered a politically exposed person. If the natural person Client is considered 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. If the natural person Client is considered a politically exposed person, the declaration must contain the information regarding the source of the financial instrument. The provisions of the Anti-Money Laundering Act relating to politically exposed persons shall also apply to the family members and the persons closely related to the 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 or copies thereof (or – based on an agreement to this effect – the authentic electronic document(s) complying with Sections 195, (1)-(4) and (8) of the Code of Civil Procedure), the validity of which must be verified by the Bank:

4.3.1. in the case of a 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);

4.3.2. foreign natural persons shall show their passport or personal identity certificate, provided that this contains authorisation for their residing in Hungary, or else a residence permit or a permit containing authorisation for residence.

4.3.3. 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.

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

4.4.1. the Client's family name and first name

4.4.2. family name and first name at birth;

4.4.3. address or, in the absence thereof, place of residence;

4.4.4. place and date of birth;

4.4.5. nationality;

4.4.6. mother's maiden name;

4.4.7. type and number of identification document;

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

4.5.1 it has been authenticated by a notary or a Hungarian representation abroad, 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 "apostille" 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 apostille 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 apostille is not stipulated by an international contract, the Bank may declare that it only accepts documents furnished with an apostille.

4.7.2. The Bank – in the interest of compliance with the statutes (including, without limitation, the Anti-Money Laundering Act and Decree 81/2006 (EC) of the European Parliament and of the Council (EU) on Information on the Payer 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 of the Client, to the Paying Party and to persons and organisations related to or in partnership with the Client, a request for information in connection with the actual activity of the Client, of the Paying Party and of the persons and organisations in 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 consistent with the data of the Client that is available to the Bank on the basis of the legal regulations.

4.12 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 customer due diligence measures by 26 June 2019, and the results of the customer due diligence are not fully available with respect to the Client.

5.2.5. Special consents

a) Automated decision-making

On the basis of the legal ground set out in section 5.2.1, the Bank shall be entitled to evaluate the Client's personal data as well as its data classed as bank or securities secrets solely through automated data processing, and to make a decision by way of automated data processing, for the purpose defined and communicated with the Client when the automated data processing was ordered.The Client shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The above provisions shall not apply in the event that the decision:

a) is necessary for entering into, or performance of, an agreement between the Client and the Bank;
b) is authorised by Union or Member State law to which the data controller is subject; or
c) is based on the Client's explicit consent

In the cases referred to in sections (a) and (c), the Bank shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Bank, to express his or her point of view and to contest the decision.

9.1. Ordinary termination

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

9.1.1. by the Client, without explanation, with a 15-day notice (in the case of Credit or Loan Agreements, with a 30-day notice).

9.1.2. the Client is entitled to terminate the Framework Agreement without explanation, with a 1-month notice period.

9.1.3. by the Bank, without explanation, with 30 days' notice of termination (in the case of a safe service, with a notice period of 15 days), with the proviso that the Bank may not terminate a fixed-term Credit and Loan Agreement with regular notice.

9.1.4. The Bank is entitled to terminate the Framework Agreement (including the CIB Mobilbank Service constituting an integral part of the Framework Agreement) without explanation, with a 2-month notice period.

14.4.3. With regard to Section **Error! Reference source not found.** *(Other forms of notification, electronic connection),* the Sensitive Payment Data and Electronic Services:

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, in the case of Debit Bank Cards, the Bank Account Holder(s) or, in the case of Credit Cards / Shopping Cards the Main Card Holder 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.

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, in view of the fact that the use of the cash-substitute payment instrument does not, in itself, prove that

- the Client has acted fraudulently, or
- has approved the payment transaction, or
- the Client has wilfully or grossly violated its obligation of safeguarding the personal authentication data, or
- the Client has wilfully or grossly violated its obligation of immediate reporting in the event that it detects the loss, theft or unauthorised or unapproved use of the cash-substitute payment instrument.

Based on the foregoing, the Bank, taking into account the result of the individual investigation, considers the following as cases of 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 (wilful misconduct, gross negligence);
- failed, late or incomplete fulfilment of the obligations related to Blocking (wilful misconduct, 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 – until proven otherwise – the time registered by the Bank shall be definitive. 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 Bank's Specific Business Regulations pertaining to Bank Cards for Consumers are supplemented with the following sections.

1.10.8 With regard to the time of the blocking request – until proven otherwise – the time registered by the Bank shall be definitive.

1.17.11. The Bank is exempt from liability stipulated by law 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 Internet-based Electronic Services for Consumers and Sole Traders are amended as follows.

20.2. Requesting the service and concluding, amending or terminating the agreement

The Service can only be requested via the CIB Bank Mobile Application and only by Clients classed as consumers. Also, the modification of the range of the accounts involved in the service as well as the termination of the service is only possible via the CIB Bank Mobile Application.

This agreement for the Service is concluded for an indefinite term. The Client may terminate the service at any time, with immediate effect, via the Mobile Application. After the Service has been terminated, the Bank will immediately terminate the provision of the Service with respect to all the bank accounts / bank cards affected by the Service.

The Bank is entitled to terminate the Service without explanation, with a 2-month notice period.

The CIB Info service is a part of the CIB Bank mobile application, it may not be separated from it, and thus the Service automatically terminates upon termination of the CIB Bank mobile application service.

CIB Bank Zrt.

Date of publication (displaying): 29 June 2018