Announcement of Changes to the Framework Agreement on Personal Credit Cards as of 20/04/2022

In keeping with Article 26 of the Payment System Act (OG No. 66/18), we are notifying our clients, Holders of personal Mastercard and/or Visa credit cards with RBA of the intended changes to the Framework Agreement that include changes to the following documents to be implemented as of 20/04/2022:

1. PI Business Fees (hereinafter: Fees)
2. General Terms and Conditions for issuance and use of the international Personal Mastercard credit card and/or Visa credit card and General Terms and Conditions for issuance and use of the Visa Iris Fashion credit card (hereinafter: General Terms and Conditions)

Fees and the General Terms and Conditions valid as of 20/04/2022 as well as the Announcement of changes to the Framework Agreement are available on the official web site of the Bank www.rba.hr and at the Bank's branches.

Below follows detailed information on changes to the Fees and the General Terms and Conditions.

1. Changes to the Fees

Changes to the Fees are as follows:

- The Bank defined deposit limits at ATM's featuring the cash deposit functionality, and in keeping with the mentioned change, the SPECIFICS OF FEE CALCULATION AND COLLECTION were updated. The Section **Card Banking Fees** was amended as follows:

Cash Deposits by Debit and Credit Cards at Bank's ATMs

Total maximum daily cash deposit limit per client is HRK 100,000.00. An ATM cash deposit can be executed only in the kuna, to any kuna payment account held at the Bank, for which the Client has been authorised to manage assets, and which account is not blocked, to a credit card account and to a loan account at the Bank. Such an order cannot be executed to a Protected Account.

- The tariff item F2.3.5.4.6., referring to ATM cash deposits by credit cards, was defined more precisely.

The current definition of the tariff item is that it is not applicable, and the new definition reads "free of charge".

2. Changes and Amendments to the General Terms and Conditions

Changes to the PI General Terms and Conditions are in several items, as follows.

In Section **DEFINITIONS,** sub-section **EFT POS Device** and **Contactless Payment**, the provision related to mandatory signature on the slip was added, which refers to a credit card with the signature strip.

- **EFT POS Device**
  The abbreviation refers to Electronic Funds Transfer Point of Sale – a terminal as a Sales Venue intended for execution of payment transactions for cashless payment of goods and/or services or cash withdrawal, which are executed electronically, and which can, depending on the respective system, require authentication by PIN, signature, swiping the card or another payment instrument against the device featuring this functionality.

  As regards individual EFT-POS devices, the payment slip must be signed, and the signature must be identical to the signature on the card with signature strip.

- **Contactless Payment**
  The payment transaction authorized by swiping the card against the POS/EFTPOS device. Depending on the amount of a payment transaction, as well as on the functionalities of the POS/EFTPOS device, authorization can be executed by merely swiping the card against the device, or by swiping the card against the device and signing the payment slip or entering the PIN.

For certain types of EFT-POS devices, it is necessary to sign a slip, and the signature must be identical to the signature on the card with signature strip.

In Section **1. CREDIT CARD ISSUANCE**, provisions on issuance of a credit card without signature strip were added and the clarification that the previously issued cards with the signature strip shall be valid until the last day of the month indicated on the card, and the Holder is obliged to sign them, and such card is invalid if unsigned

- The bank issues Credit Cards without a signature strip. Credit cards issued with a signature strip are valid until the last day of the month indicated on the card in accordance with the provisions of these General Terms and Conditions, and the Holder is obliged to sign them, and such card is invalid if unsigned, and the Credit Card Holder assumes full responsibility for the damages due to an unauthorized person using the Credit Card in the case the unsigned Credit Card is lost or stolen.

In Section **4. SPENDING LIMIT**, the provision on the Holder's obligation to make the payment with the option of executing the payment also on the first following working day after a non-working day or holiday was added.

- The Holder shall make the payment by the maturity date given on the Credit Card Statement at the latest by executing the payment to the Bank's account or/and by contracting a direct debit for their current or FCY account with the Bank (as stated by the Holder in the Application). If the maturity date is not a working day, the Holder shall make the payment on the last working day before the maturity date at the latest or the first following working day.

In Section **5. USING THE CREDIT CARD AND THE GRANTED SPENDING LIMIT**, the provision on rules for executing a cash deposit transaction on the Bank's ATM's, on the maximum daily limit, deposit currency and possible types of payment was added.

- A credit card can also be used to execute a cash deposit transaction at the Bank's ATMs that support such functionality. Cash deposits at ATMs are allowed within the maximum daily limit set by the Bank. Cash deposit at the ATM can be made only in HRK, to the Bank's account for the purpose of settling credit card obligations or credit card loan obligations, as well as to any kuna payment account opened with the Bank under which the Credit Card Holder has the right to dispose and which is not blocked, except for the protected account.

In Section **6. CONSENT FOR PAYMENT TRANSACTION EXECUTION** details were provided with regard to the tools for input of the one-time password created by the current tool (mToken, card reader, Token)

- entering security elements required by the respective sales venue when buying goods and services on the Internet, and if the respective Internet sales venue requires also additional entry of a one-time password created on the existing device (mToken, card reader, Token) for access to online banking (RBA Internet and Mobile Banking).

In Section **12**. **NOTIFICATION AND COMPLAINTS** the manner for submitting notifications or complaints in connection to unauthenticated, irregularly initiated, unexecuted and/or irregular or delayed transactions was updated

- All notifications or complaints with respect to payment transactions that are unauthorized, not properly initiated, not executed and/or not executed properly or delayed transactions can be sent to the Bank by the Credit Card Holder in the following manners:
  - by e-mail to the address: prigovori@rba.hr
  - in person at the RBA Branch
  - through the Internet / Mobile Banking
  - by post to the address: Raiffeisenbank Austria d.d., Complaints Management, Magazinska cesta 69, 10000 Zagreb.

  The complaint can be submitted on the form available on the Bank's official website www.rba.hr

In Section **13. CREDIT CARD PROTECTION – LOST AND STOLEN CREDIT CARD**, the following was amended:

- obligation of the Holder to sign a credit card with signature strip was added:
  - sign the Credit Card with signature strip;
- precisely stating the information about the card and its security features and tools for online banking access that are governed by the prohibition of allowing access to other persons:

- not communicate any of your personal data, and especially not the identity card number, personal identification number (OIB), passport number, etc. or information of the card (card number, validity date, other security features, such as one-time password, security code, control number, etc.) and data about Online Banking access devices used for authentication (e.g. Serial Number of Token or mToken) on unverified web browsers, in telephone calls with unknown or unverified persons, or in replies to unverified e-mail messages or through other Messaging Applications (e.g. WhatsApp, Viber, etc.);
- not respond to e-mails or telephone calls requesting Personal or Card or Authentication information from the Credit Card Holder and not download suspicious documents from the web;

- provision whereby the Bank is authorised to block a payment instrument if it suspects possibility of breach of the provisions of the regulations regulating prevention of money-laundering and terrorist financing if the Holder, at the Bank's request, fails to deliver the required information and documentation which are, in compliance with the regulations regulating prevention of money-laundering and terrorist financing and/or the Bank's general acts passed pursuant to these regulations, required to establish and/or continue a business relationship
  - if it finds or suspects possible violation of the provisions of regulations governing the prevention of money laundering and terrorist financing, and if the Credit Card Holder does not submit the required data and documentation in accordance with applicable regulations on prevention of money laundering and terrorist financing and / or general acts of the Bank adopted on the basis of these regulations, which are necessary for the establishment and / or continuation of a business relationship

If you do not agree to the proposed changes to the Fees and General Terms and Conditions, you can terminate the Framework Agreement without any charges with legal effect of notice on any date prior to the changes coming into force.
If you do not notify the Bank of terminating the Framework Agreement by the proposed date of the above changes coming into force, it will be deemed that you have accepted the changes.

Yours sincerely,
RBA