VISTA BANK

Security recommendations for using the card

General security rules regarding the card and the PIN code

- Check the integrity of the envelopes containing your card and/or PIN code. Please inform the bank immediately if you have any suspicions.
- **Never keep the card together with the PIN code.** Do not write the PIN code on the card or on any paper kept together with the card
- Change at an ATM the initial PIN code received from the bank OR memorise the PIN and destroy the paper with the PIN code imediately afterwards.
- Do not expose the card to electromagnetic sources, including mobile devices (phone/tablet). They may affect the card's chip functionality.
- Do not hand over your card and PIN to be used by other people.
- Do not provide the card number, CVV/CVV2 codes, expiry date to anyone, even if the request **seems to be** from legit sources such as bank, police or law enforcement entities. **Neither the bank nor other institution will ever request you these information.**
- Regularly check your account statement / card activity report, at least monthly, and immediately report any identified discrepancies to the bank.
- Contact the bank's Call Center immediately (the phone number is displayed on the bank's website) and block the card if you have lost it, cannot find it or suspect that it has been duplicated / cloned in any way.
- **NEVER provide information about your card or bank details when requested by e-mail, telephone, SMS or other electronic means of communication**

  Be very careful when receiving e-mails asking you to disclose data about your card, as it is very possible that they are Phishing attempts (fraudulent attempts to obtain personal data).

  Phishing messages may request you to update, confirm, or enter card details, such as card number, expiration date, CVV / CVV2 codes, payment authorization password, One-Time Passcode (OTP) payment codes sent via SMS, or other personal information, by accessing a link that will redirect you to a fictitious site. Both the address from which the e-mail is sent and that of the destination site may resemble those of a trusted institution / company, but a closer look at the URL / address of the phishing website may reveal that at least one letter is different (example: goo.gle.com instead of google.com). Sometimes these messages contain grammatical errors, being automatically translated from other languages and sent to a large number of cardholders.

  In such cases, do not click on the included links and delete the message. Notify the Bank, as well as CERT-RO regarding any phishing message or phishing site you discover.

  An example of phishing: you receive an email informing you have won a trip abroad and all you have to do to receive the travel voucher is to enter (on a site similar to that of the bank or a trusted merchant) the following information to confirm your identity: your name, address and card details.

  Also, such requests can be sent by SMS (SMSishing) or by phone (vishing = voice + phishing).

  An example of vishing: you receive a phone call from someone who claims to be an employee of the bank and wants to verify the card number, PIN code or security code because a security alert has been initiated.

  Vista Bank will never ask you to transmit, confirm or update card data by accessing a link sent by e-mail or SMS, respectively by telephone conversations.

VISTA BANK

Security rules for using the card at ATMs

- Visually check if you find anything unusual or suspicious about the ATM. If it appears to have devices attached to the card insertion slot or keyboard, do not use the equipment. Cancel the transaction if you have already initiated it and leave the location. Never try to remove the suspicious devices. In this case, notify the bank immediately so it can undertake the necessary checks.
- Protect the visibility of the PIN code during the entry, by blocking the view of others, standing close to the ATM and protecting the keyboard with the other hand.
- Whenever possible, use ATMs in well-lit areas with good visibility.
- Make sure the other people in line are at a reasonable distance from you.
- Do not accept the help of strangers who offer to "help" you when the ATM has certain errors.
- Avoid opening your purse, bag or wallet while waiting in line. Secure the cash as soon as you receive it.
- Do not let your attention be distracted while operating the ATM.
- Make sure you have recovered the card from the ATM and, if applicable, the requested cash.

Security rules regarding the use of the card at physical merchants (payment at POS)

- Protect the visibility of the PIN code when you type it on the POS keyboard (cover the POS keyboard with the other hand or with an object when typing the PIN).
- Keep the card in your possession at all times and do not hand it to anyone even if you were asked to do so by the sales representative (cashier, waiter, etc.).
- When you have the card in your hand, make sure that no one sees the CVV code digits on the back of the card.
- For each transaction, approved or rejected, you must receive a receipt (which you keep with you).
- Make sure you have the card before leaving the commercial location.
- Keep the contactless card in an aluminum foil (or in special covers that keep the contactless cards safe) when you don't need to make a payment at POS. Thus, you protect your card from ill-intended people who might place near your contactless card a fraudulent POS and thus withdraw small amounts (up to 100 Lei) for which PIN authorization is not necessary. Make sure you have activated the SMS Alert service to receive SMS notifications with the amounts and merchants where your card payments have been authorized. If you do not recognize a transaction as authorized by you, please notify the Bank immediately. (NOTE: The SMS Alert Service is activated at your request in any Bank branch).

Security rules for card usage at virtual merchants (e-commerce / internet transactions)

- Before you perform an e-commerce purchase make sure the site is Visa Secure certified (Visa Secure logo is displayed on the merchant's site).
- Try to find out in advance, from different sources, information regarding the trustwhorthyness of the virtual merchant
- Learn how to recognize the signs of connection to a secure site: connection via https: // (from the URL of the website) and a website valid certificate.
- Read carefully, BEFORE making / completing a transaction, the merchant's policy regarding transaction processing and cancellation, delivery of products / services, etc., to avoid post-transaction litigation as much as possible.
- Enroll your card and use the bank's mobile e-commerce application for authorizing online card transactions (Vista 3D Secure), for mobile devices with Android and iOS.
- When using the mobile e-commerce application for authorizing online card transactions (**Vista 3D Secure**) offered by the bank, ALWAYS read carefully, BEFORE approving the transaction by secure means specific to your mobile device (biometric identification, other methods), the defining elements of the transaction, such as the **name of the merchant, the value of the transaction, the currency of the transaction, etc**., as the case may be.

- **Never enter the card PIN code on Internet sites** (the PIN is required only at the ATM or POS, and the Bank will never ask you to communicate the card PIN on Internet sites).
- Protect your personal computer and mobile devices: use antivirus programs and update them periodically. Do not open the e-mails attachments received from strangers and do not click on links. Do not install non-certified programs and applications.
- Do not use a computer that does not belong to you (eg at the Internet Café, at the hotel, at "friends", etc.) when initiating online card transactions, because that computer may already have malware installed that can steal your card data and payment authorization codes.