The Card Instrument: Utilization Rule and Recommendations

Interpretation of Terms

- **Card Instrument** – a payment instrument, including a payment card, mobile phone, computer etc. high-tech, with an integrated payment application by means of which a payer may initiate a card transaction;
- **Bank Card (hereinafter – Card)** – the payment card owned by the Bank and generated for the client, which is designed for effecting various bank operations by the client (the Visa or MasterCard issued by the Bank).
- **Virtual Card** – the unity of card details (at least its number, validity term and the safety code) by means of which the card owner may affect payments with due regard to the authentication measures.
- **PIN code** – personal identification number, i.e. the four-digit password.
- **CVV code** - the three-digit card verification code on the reverse side of the card.

The Key Safety Rules

- While taking your card at a Bank service center make sure that the **PIN code** is placed in an envelope which should not be damaged or open so that the **PIN code** is visible to the others. If the envelope is damaged or opened contact the Bank call center (+ 995 32) 2008080 / cell phone: * 8080
- Remember the **PIN code** and destroy the envelope.
- It is recommended to change the **PIN code** by a combination of digits of your choice by using the ATM of the Bank service center.
- If you are unable to remember the **PIN code,** do not keep it in writing together with the card or inscribe it on it. The **PIN code** in writing should be kept out of the reach of third persons (friends, relatives, family members)
- Having received the card at a service center, sign it in the relevant field on the reverse side.
- Never tell the third persons (friends, relatives, family members) the whole card number, validity term, **PIN and CVV codes.** Be especially careful if you are asked for the said information by phone, e-mail or social networks etc. Do not disclose the information if the person asking for it has introduced himself as a Bank employee. In such cases, contact the call center of the Bank (+ 99532) 2008080 / cell phone: *8080 to report the incident.
- Pay attention to e-mails received at the office or personal e-mail address. Never click the links specified in a suspicious e-mail message if the sender asks for your card number, **PIN or CVV codes,** the memorable word, the internet bank user's name, password etc. confidential information. Not infrequently, from links you are forwarded to the web-site used for unsanctioned obtainment of information.
- Please mind that the Bank never asks its clients to supply confidential information by e-mail or etc. communication means.
- Remember, the card is the means to manage your account. Therefore, in case of sharing your **PIN code** with third persons or loss of the card, unsanctioned use of your money resources by third persons is probable.

- If you suspect that third persons learned your card **PIN code**, number, the validity term or **CVV code,** or you have lost the card, contact the Bank immediately (+ 99532) 2008080 / cell phone: *8080. A call center employee will help you take the relevant measures.
- Do not allow third persons to copy or take photo of your card. Never send your scanned card by e-mail or the so-called Messanger or share it by the social media.

The Card Use at ATM

- While using an ATM, make sure that there are no extra devices installed on it. Special attention should be paid to the **PIN code,** keyboard and card slot. If you notice the wrongly installed keyboard or the so-call skimmer on the card slot, you'd better find another ATM. Report your suspicion to the Bank the ATM belongs to by dialing the phone number usually inscribed on ATMs.
- While typing the PIN code, cover the keyboard so that the people standing next to you are unable to see it. Please, take into account that if the **PIN code** is typed wrongly several times, the ATM will retain the card.
- Immediately upon completion of the transaction, remove the card, cash and the receipt. Count the sum of site, make sure that the ATM returned your card, wait for the receipt (if requested) then place the sum and the card in a safe place (a bag, wallet) and leave the ATM.
- Never use the card in the ATM by following third persons' instructions given by phone. Do not allow outsiders to get involved in your transactions and take care if a stranger advises you how to use the ATM.
- It is recommended to keep receipts of the transactions effected by ATM to compare them with the bank statement.
- If the ATM retains your card, contactvthe Bank immediately: (+ 99532) 2008080 / cell phone: *8080

Card Use at Outlets

- In the settlement by clearance used the card only at reliable outlets.
- To minimize the risk of unauthorized access to your card data, the transaction should be effected in your presense. Do not let an outlet or service station staff take the card away.
- In case of card settlement, an outlet or a service station employee may ask you to produce your ID, to type the **PIN code** on the POS terminal or/and sign the receipt. While typing the **PIN code** make sure that no-one sees it. If the POS terminal is not equipped with the keyboard protection device, cover it while typing the **PIN code.** Before signing the receipt (if requested) and leaving the outlet or the service station, check if the sum on the receipt is the same as the transaction sum.
- If the POS terminal rejects a transaction, keep the rejection receipt to compare it with bank statement.
- In some outlets and service stations, you may be asked to put your bank card through the card reader installed on the keyboard, which is not certified by (Visa, MasetCard) card payment systems. Ask the outlet staff if they are going to put your card through another device apart from the POS Terminal. If so, warn them that they may use a specially

handed over so-called test card that will allow them to complete the payment while your confidential data are not stored in dubious device.

The Internet Card Use

- In online trading, use only the well-known the reliable sites. In case of even a slight suspicion about the reliability of the website, you can verify the address at: http://www.scamadviser.com
- Do not use the **PIN code** for online transactions. The card number, validity term, name, surname and **CVV code** of the card holder will do.
- For the Internet transactions, it is recommended to use a separate card (e.g. a virtual card or an e-card) where the money resources are placed as required, immediately before the transaction.
- Always pay attention to the address of the website you are posting your card data on. Some addresses may be transformed deliberately (several symbols changed) for unsanctioned access to your card data. You can check the validity of the website by checking its certificate (generally by clicking the padlock icon).

Verification of the Website Certificate

- In online trading, it is recommended to use your PC or a mobile device to minimize probability of disclosure of your confidential information.
- In online trading, do not use public or unfamiliar Wi-Fi.
- If while effecting online transactions you use common access or another person's computer, do not save the card data and delete them upon completion of the transaction.
- Be sure to have an anti-virus software installed on your PC or mobile device. To reduce the risks of the virus penetration into your PC, regularly update the anti-virus software operational systems of the device etc. software.
- Familiarize yourself with the Bank's cyber security information at: https://www.cartubank.ge/ge/612/