HSBC

Security rules for using ATM and Credit Cards

HSBC Bank Armenia cjsc (hereafter the Bank) credit and ATM cards provide you a fast, convenient and reliable way to make cash withdrawals or pay for your purchases anytime and anywhere. To protect your credit and ATM cards from fraud and unauthorized use when using them at home or abroad, You should ensure the following security rules as a minimum:

1. **Make sure to sign the back side of your card (applicable to credit cards only) with a ball pen immediately after you receive it.**

2. **Do not allow anyone else to use the card.**

3. **Do not disclose card related data such as Card Number or expiry date to third parties, including by email, and ensure that all transactions are conducted in Your presence.**

4. **Never pass Your credit or ATM cards to anyone else or allow anyone to have access to your cards. If a credit or ATM card is taken by a family member (spouse, child, and parent), with or without Your knowledge or consent, You are responsible for their purchase or other transactions.**

5. **Do not leave Your card unattended in a public place.**

6. **Immediately report about Your lost or stolen cards, as well as any suspicion related to any transaction made by Your card, to the Bank.**

7. **Never tell Your Personal Identification Number (PIN) to anyone, not even Bank employees.**

8. **Remember that Bank will never request you to provide Your card's PIN and/or CVV/CVC details (the 3-digit security code on the back of your card).**

9. **Do not use repetitive digits (like 2222, 1111, etc.), consecutive digits (like 1234, 6543) or easy to guess personal data (for example birthday, phone number) when changing Your PIN.**

10. **Do not keep record of Your PIN together with Your card even if it is disguised as a telephone number. This can be easily deciphered.**

11. **Do not store Your personal card details on Your computer or other electronic devices or electronic databases, especially PIN and/or CVV/CVC details (the 3-digit security code on the back of your card).**

12. **If the ATM or POS terminal You are using does not have a protective shield to cover the number pad, always use Your hand as a shield while entering Your PIN to keep it a secret.**

HSBC

13. If you realize the ATM has been tampered with or there is other device on ATM after You have inserted Your card, immediately contact the Bank while still standing at the cash machine if it is safe to do so.

14. Be wary from any person offering assistance when you use the ATM, especially if you have not requested such assistance and the person is not a Bank employee.

15. If You have a suspicion that Your PIN and/or any sensitive information (e.g. card details) is known to someone else, immediately inform the Bank.

16. Contact the Bank immediately if somebody on behalf of the Bank requests You to provide Your card, PIN or other personal information.

17. Before effecting any transaction over the Internet, go through the terms and conditions for making a transaction and payment in details, by paying special attention to parts printed in small letters.

18. Before effecting a purchase, hotel or car rental reservation over the Internet, search for reviews or forums related to product or service to confirm whether the merchant can provide what is promised on the website.

19. Make sure that the receipts are provided after each transaction.

20. Always check transaction receipts, purchase amounts reflected thereon before signing them.

21. Keep the transaction and ATM receipts to reconcile them against monthly statements.

22. Always check the card(s) statement(s), especially after travelling. Check the purchase amounts against transaction receipts, as well as transactions made by Your ATM card with the transaction amounts stated in the statements, and in case of detecting any unauthorized or invalid transactions immediately notify the Bank.

23. Destroy the financial documents, including credit card transaction receipts, ATM transaction records, credit card and Bank statements, if no longer needed.

24. Ensure the Bank is provided with Your up to date contact details before travelling abroad. Particularly Your mobile phone number and email address.

25. Pay attention to card expiry dates. If You haven't received the renewed card yet, contact the Bank to receive Your new card.

26. When performing 3D Secure transaction always check whether the partially hidden mobile number is true and only than request to send password via SMS.

27. Always check whether the transaction's amount and the merchant are true in the received SMS notifying the transaction.

Important note: *Upon signing the agreement the subject terms to be provided to customer by the financial institution.*

Note: In case of discrepancies between the Armenian and English versions of this page, the Armenian version shall prevail.

Last updated on: 16/02/2019 15:00