Changes in the online card payment!

Dear Customer,

Please be informed that in line with the legislation our Bank is introducing the Strong Customer Authentication[1] **for the online card payments** probably from December 17, 2020 but no later than January 1, 2021. Once introduced, it will not be enough to provide bankcard data to approve online purchases; the **authentication takes place in two steps**, thus confirming the fact that the transaction was indeed initiated by the cardholder. This process serves the protection of your bankcard information and prevent possible fraud.

To authenticate the transaction the following **additional two factors must be submitted** besides the card data:

- Secure internet payment control **SMS code**
- **Password**

The Secure internet payment control SMS code:

is used **first in the authentication process**. It is a randomly generated sequence of numbers sent via SMS message which must be submitted during the payment – upon request – on a secure homepage of the bank separated from the merchant's site. The Secure internet payment control SMS code is not static, new code is generated and sent* via SMS for the cardholder for each online purchase transaction.

As a **second step the Password** must be submitted on a banking secure homepage separated from the merchant's site.

Our Bank will send the cardholder's **Password** - that must be used for online payment authentication - in SMS **during December 2020**. The Password is a randomly generated six digits sequence of numbers.

Password:

- belongs to the cardholder, can be used for each card of the cardholder issued by our Bank, so if the cardholder has more KDB cards issued for his name, the same Password must be used. There is no possibility to set different Password for different cards of the same cardholder.
- can be modified via Call Center (+36 1 473 4440)
- can be re-generated in case of lost or forgotten
- expiry date is 5 years, so the Password shall be changed in each 5 year.

Beside the Password an additional code will be send in the same SMS to the Cardholders, called Client Identification Code (CIN Code), which is a nine digits sequence of numbers needed for the Password change via Call Center if necessary.

---

[1] *Strong Customer Authentication, SCA is prescribed by the EU 2015/2366 directive (called PSD2). Designed to decrease the e-commerce related fraud issues and cheatings. The main modification from 1st January 2021 is that the financial institutions must use at least two factor from the next three to authenticate the online payments:*
- Knowledge/information, Something what is known only by the Cardholder, in our case it is the Password;
- Possession, something only the user possesses, in our case it is the mobile phone where The Secure internet payment control SMS code is delivered;
- Inherence, biometrics of the cardholder e.g. fingerprint.

*The Password to be used for secure online payments will be delivered for the Clients having KDB Mobile Kontakt service (Bankcard security SMS, Mini SMS, Full SMS) attached to the bankcard or to the account which the card is linked to at the date of Password sending.

If You do not have KDB Mobile Contact service, please apply it as soon as possible via KDB NetBank, Call Center or personally in our Branches, because after the release the online card payments will be declined at those merchants which are using strong customer authentication.

The online payment's process:

Actually:

1. submitting card data (card number, expiry date, CVV) on the Merchant's or on the acquirer bank's site
2. transaction finalization (approve with the order/submit… bottom)

From Strong Customer Introduction date (probably from December 17, 2020 but no later than January 1, 2021):

1. **submitting card data (card number, expiry date, CVV) on the Merchant's or on the acquirer bank's site,**
2. **submitting the Secure internet payment control SMS code – received at the transaction initiation – on a banking secure homepage separated from the merchant's site,**
3. **submitting the Password on a banking secure homepage separated from the merchant's site,**
4. **transaction finalization and redirecting to the merchant's site.**

Please follow our homepage we inform you about the exact date on the front page.