

Dear Merchant Partner!

We would like to inform you that **as of September 30, 2020**, the rules of strong customer authentication (PSD2) must be applied by all **webshops** and **merchant websites** that provide online card payments.

In the following, we would like to draw your attention to the related information and **related tasks**, which also affect our Bank's vPOS service.

What is strong customer authentication?

Strong Customer Authentication (SCA) is an additional security check step for card payments and electronic payment transactions that took effect on September 14, 2019. Strong customer authentication ensures that wherever a purchase or banking transaction is made, only the person authorized to use the card, ie the cardholder, can authenticate the transaction. According to the European Union's PSD2 directive and the regulations of the card schemes (Mastercard, VISA), **from 30 September 2020**, strong customer authentication will be required for online bank card purchases to identify the cardholder. Based on the above, strong customer authentication and related technical regulations should also be applied when initiating payments in webstores.

How does the payment process change on the Internet?

- The customer can identify himself during the payment by entering the code received in the SMS and the password received from his bank, but even with his phone's fingerprint reader or face recognition (eg Face ID).
- It is up to the card issuer to decide which of the identification options to choose and whether to apply exception handling rules.
- The acquiring bank must ensure that the above process can be fully implemented in the case of card payment transactions in the webshops.
- In order to apply the exception management rules in accordance with the PSD2 guidelines, issuing banks will in future have to have more information about the given transaction than before, which information must be transmitted in the transaction data during the online purchase.

What are the merchants', your tasks to keep your customers paying smoothly?

In accordance with the requirements of the card schemes, our bank will implement the requirements related to the strong customer authentication process in your webshop by the date indicated above, but in order to operate in accordance with additional PSD2 guidelines for exception management rules, and allow issuer banks to apply exception rules upon their decision, you must also make changes to the operation of the online webstore (vPOS) described in the [UniCredit vPOS 3DSecure Additional Data](#) document available on our website. Full documentation is available here: [Developers' Guide](#).



What else is changing?

The domain name related to UniCredit Bank's vPOS service will be also modified. For technical information about the domain name change, see the related document [UniCredit vPOS URL Change](#) uploaded on our website.

Along with PSD2 compliance, the Mastercard SecureCode and Verified by Visa logos will also change, which will also need to be replaced to the Mastercard ID Check and Visa Secure logo, which indicate increased card data security, and shall be placed next to the card schemes' brand logos. The [MC ID Check logo](#) can be downloaded from our website here and the [VISA Secure logo](#) can be downloaded here. Please also check the Mastercard and Maestro logos to ensure that they appear in your web store according to the current applicable versions. The [Mastercard logo](#) can be found on our website here and the [Maestro logo](#) here.

What happens if the above changes are not applied by the webstore?

If the above changes are not implemented in your webshop **by 31 December 2020**, the Bank is not entitled to receive and process payment transactions initiated in the webshop after this date.

Please ensure that the changes contained in both documents indicated in this letter are implemented by the above deadline so that you can provide online payments to your customers smoothly after this date in the future.

We will also forward this letter to the development contact indicated in our contract:

If there is a change in the developer's details, please notify your relationship manager immediately.

If you have any questions on the above or need technical support, please feel free to contact our colleagues at ecomm@sia.eu.

Regards,
UniCredit Bank Hungary Zrt.