

MARCARD, STEIN & CO

Bankiers

INFORMATION ON IMPLEMENTING THE REVISED EUROPEAN PAYMENT SERVICES DIRECTIVE (PSD II) BY 14 SEPTEMBER 2019

What does the introduction of the Second European Payment Service Directive (PSD II) on 14 September 2019, mean for you in real life?

We want to give the current state of affairs and keep you up-to-date on what will change for you.

The new payment transaction guidelines offer more transparency, convenience, flexibility, and security for your banking needs.

This requires banks and payment service providers to make some technical and contractual adjustments reflecting the new regulations.

We have already implemented the contractual part by sending you the new terms and conditions on 8 July of this year.

What is the revised European Payment Services Directive (PSD II)?

PSD II is an EU Directive to improve security in European electronic, online, and card payments.

This includes regulations for providers external to the customer-bank-relationship offering account and payment services.

The directive furthermore requires new conditions and processes for a strong customer authentication in online banking and online card payments.

What does the revised European Payment Services Directive (PSD II) mean for you as a bank customer?

- Uniform European legal and technical standards for online access to existing bank accounts by third-party providers;
- Introduction of a general two-tier authentication for online account access;
- Online card payments now require two authentication media for validation.

What is a strong customer authentication?

On 14 September 2019, it will become mandatory to use a strong customer authentication. That means bank customers must identify themselves from this point forward for their online banking activities and card payments with at least two of the following three authentication elements:

- Personal identifying feature (e.g. biometrics like fingerprints)
- Personal security credentials (e.g. PIN)
- Code generated by an object in the customer's possession (e.g. TAN via token or smartphone)
- You are already using a two-tier authentication in your payment transactions (see PIN/TAN process).

MARCARD, STEIN & CO

Bankiers

From 14 September 2019 onward, when logging into your online banking account or accessing sensitive personal data within the online banking system, you will be prompted to enter - in addition to your PIN (personal security credential) - a TAN (code generated by an object in the customer's possession) or a biometric feature (personal identifying feature).

There will be no immediate changes for card payments in supermarkets or at store cash registers.

- Online card payments will from mid-September onward require that you authenticate the transaction to the online vendor with two elements.
- You may authorize your payment via a banking app or text-based TAN.

What are third-party providers?

Third-party providers are external service providers who use bank infrastructures without operating any themselves.

The new directive differentiates three categories of such providers:

- **Payment initiation services**

In this case a customer requests that the service provider makes an online payment transfer charged to the customer's account at his or her bank. This may be to pay for an online purchase on a vendor's website.

- **Account information services**

Customers may use these services to retrieve account information like pending transactions, concluded transactions, and balances. The customer needs to establish an online banking account for this. This is a practical option if you maintain accounts at different banks and wish to get a comprehensive overview of your finances and/or accounts.

- **Card issuers**

Card issuers offer bank-independent payment cards. With your consent, the issuer will check funds availability with your regular bank when making a payment that you initiated with such a card.

What data at your bank may these service providers access?

You as the customer decide what account data a third-party provider may use or view for its services.

MARCARD, STEIN & CO

Bankiers

What will change in your access to Marcard, Stein & Co online banking?

On 12 September 2019, we will introduce two-factor authentication for logging into your online banking account as mandated by the Second European Payment Service Directive (PSD II).

Simultaneously the time out limit for browser-based online banking from currently 20 minutes is changed to 5 minutes per online banking session. That means the system will automatically sign you out if you have not performed a system action for 5 minutes within a single online banking session.

If you are using dedicated online banking software like windata or StarMoney to access Marcard, Stein & Co online banking, these changes will not affect you.

Our service hotline will gladly answer any questions you may have toll-free within in Germany at 0800 72 33 982 and internationally at +49 201 31 01 370.