11 July 2019

14 September 2019: The final deadline for compliance with PSD2's Regulatory Technical Standard (RTS)

On 25 November 2015, the Directive on payment services in the internal market, no. 2015/2366, also known as "**PSD2**", was adopted by the European parliament and Council. In the Republic of Slovenia PSD2 was transposed with the Payment Services, Services for Issuing Electronic Money and Payment Systems Act (*Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih* "**ZPlaSSIED**"), which entered into force on 22 February 2018. The Slovenian legislator implemented the provision of PSD2 into Slovenian law directly, without any modifications.

The main body of ZPlaSSIED has been in use for some time now, while provisions of Articles 117, 118, 119 and 153 ZPlaSSIED will enter into force on 14 September 2019. Said Articles of ZPlaSSIED regulate authorization of payment transactions, namely (i) Confirmation on the availability of funds (Article 117 ZPlaSSIED), (ii) Rules on access to payment account in the case of payment initiation services (Article 118 ZPlaSSIED); (iii) Rules on access to and use of payment account information in the case of account information services (Article 119 ZPlaSSIED); and (iv) Authentication (Article 153 ZPlaSSIED).

This article provides a general overview of the impact these rules have on the payment service providers (*i.e.* payment institutions, credit institutions, etc.) and the account servicing payment service providers[1] (*i.e.* banks) when performing payment services in the Republic of Slovenia, with a special emphasis on the process of strong customer authentication ("**SCA**").

The wording of Article 65 of PSD2 was implemented into Article 117 of the ZPlaSSIED which requires the bank, upon request of the payment service provider issuing card-based payment instruments (*e.g.* MasterCard), to immediately confirm whether an amount necessary for execution of a card-based payment transaction is available on the payment account of the payer (the "**Confirmation**"). However, this Confirmation is subject to specific conditions on both the payment services provider's and bank's side. The nature and use of the Confirmation are also strictly regulated by PSD2 and ZPlaSSIED. Importantly the Confirmation shall only include a simple "*yes"* or "*no"* statement on availability of funds and not a statement on the actual account balance. Additionally, the Confirmation information shall not be stored or used for any purpose other than for execution of the card-based payment transaction. And finally, the Confirmation shall not enable the bank to block funds on the payer's payment account. Also, the payer may request the bank to identify to him the payment service provider that requested the Confirmation and the answer provided.

Article 118 ZPlaSSIED (*i.e.* Article 66 PSD2) provides that a payer (*i.e.* customer) has the right to make use of a payment initiation service provider to obtain payment services. This means that under the conditions specified in this Article a payment services provider will have the right to access the payer's bank account and will be able to make a payment order directly in the payer's name. Unlike before, PSD2 and ZPlaSSIED provide the payment services provider with a secure and regulated access to the payer's bank account and the bank is completely aware which payment services providers have access to their customer's bank accounts.

Furthermore, new provisions of ZPlaSSIED provide that a payment service user has the right to make use of services enabling access to account information. This means that the payment services provider (i) shall have access to the bank account information of its customers which will be securely provided by the bank and (ii) will be able to provide their customers directly with such information, subject to the conditions under Article 119 ZPlaSSIED.

[1] Account servicing payment service provider means a payment service provider providing and maintaining a payment account for a payer (*i.e.* usually a bank).

Importantly, the provision of account information services and the provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment service provider and the bank.

The last Article coming into force on 14 September 2019 and the Article with the most profound impact for the account servicing payment service providers (*i.e.* banks) is Article 153 ZPlaSSIED (*i.e.* Article 97 PSD2). This Article covers the question of authentication of the payer (*i.e.* customer). The law provides that the payment service provider must perform SCA when/if the payer:

1. accesses its payment account online;
2. initiates an electronic payment transaction; or
3. carries out any action through a remote channel which may imply a risk of payment fraud or other abuse.

Although this new standard requires mostly technical implementation by banks and payment services providers, legal interpretation of the latter is important to ensure compliance. Strong customer authentication ("**SCA**") means an authentication based on use/verification of two or more elements that fall within the scope of:

(i) Customer's **knowledge**, *i.e.* something only the user knows; e.g. a password or a PIN code. The European Banking Authority ("**EBA**") takes the view that many other elements also comply with this criterion, however, continues that, for example, email address or username, card details (printed on the card) and OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) are not sufficient;

(ii) Customer's **possession**, *i.e.* something only the user possesses; *e.g.* a phone or a hardware token. Possession does not solely refer to physical possession but may refer to something that is not physical (such as an app); however, an app or web browser that does not ensure a unique connection with a device would not be a compliant with the possession element; and

(iii) Customer's **inherence**, *i.e.* something the user is; e.g. fingerprint or face recognition, as well as retina and iris scanning, vein recognition, hand geometry, voice recognition, keystroke dynamics (identifying a user by the way they type and swipe, sometimes referred to as typing and swiping patterns), the angle at which the PSU holds the device and the PSU's heart rate (uniquely identifying the PSU) and many other technical inventions, subject to human imagination.

The above specified elements must be independent from each other in the sense that a breach of one does not compromise the reliability of the others.

Furthermore, Article 153 ZPlaSSIED requires the payment service provider to apply SCA which includes elements of dynamic linking of the transaction to a specific amount and a specific payee, when an electronic payment transaction is initiated. The payment service providers must also establish and keep in place strict security measures to protect the confidentiality and integrity of payment service users' personalized security credentials.

In the light of the above, one of the fundamental changes introduced by PSD2 is to regulate payment security requirements under national laws. One such requirement is for the payment services providers to apply SCA to electronic transactions in instances defined above. Considering the main objectives of the PSD2 and Slovenian ZPlaSSIED, which are to (i) ensure security of electronic payments and to (ii) reduce, to the maximum extent possible, the risk of fraud[2], it is essential that the industry participants take the necessary steps to apply or request SCA and thus avoid situations in which payment transactions are rejected, blocked or interrupted. An additional goal is also to avoid potential administrative fines for non-compliance, as specified below. In my opinion, a key component for successful application of SCA is to explain and make the customers aware of such changes, *i.e.* explain that this is paramount for customers to be able to continue making (online) payments.

There is a growing concern of non-compliance as the deadline for entry into force of the relevant PSD2 and ZPlaSSIED provisions is fast approaching. A survey, done by the EBA, shows that a number of existing approaches within e-commerce providers, for card payments in particular, would not be compliant with SCA.[3] In the Republic of Slovenia such non-compliance could result in administrative fines ranging from EUR 12,500 and up to EUR 125,000, which may be applied against an account servicing payment service provider (*i.e.* the bank) or payment services provider that does not perform the required SCA when carrying out payment services in the Republic of Slovenia. The same administrative fine may also be imposed for breaches of obligations provided by Articles 117, 118 and 119 ZPlaSSIED; for example, if the account servicing payment service provider does not provide the Confirmation of available funds, if the payment service provider blocks the funds on the payer's account, etc.[4]

[2] PSD2, recital 95.
[3] European Banking Authority, Single Rulebook Q&A; URL: https://eba.europa.eu/.
[4] ZPlaSSIED, Articles 294 and 296.

Similarly, the responsible person of the account servicing payment service provider (*i.e.* the bank) or payment services provider can be fined with an administrative fine from EUR 1,250 and up to EUR 4,000.

According to the unofficial information provided by the Bank of Slovenia, which is the competent authority that conducts supervision in respect to the compliance of banks with the provisions of ZPlaSSIED in the Republic of Slovenia, there will be no transitional relief period which means that the requirements of SCA will have to be complied with immediately after 14 September 2019.

To conclude, PSD2 and ZPlaSSIED enable bank customers, either consumers or legal entities, to use third-party payment services providers as a link between the bank and the customer. At the moment, and to a greater extent in the near future, customers may use certain apps, for instance, Apple or Google services, as an interface to make online payments, payments in stores, make P2P transfers, analyze spending habits or simply to pay bills, while still having their money safely placed in their current bank account. Banks will be obligated to provide these third-party service providers with access to their customers' bank account information through open APIs, *i.e.* application program interfaces. This will enable third-party service providers to build specialty financial services on top of banks' data and infrastructure. Thus, the banks will no longer be only competing against other banks, but everyone else offering financial services. PSD2 and its national implementation acts will fundamentally change the payments value chain, customers' expectation and profitability of different business models.

Author:
Tisa Ljubetič, Junior Associate