16. Special Terms and Conditions Concerning Strong Client Authentication

version 05/2022

KB | SmartPay

1. STRONG CLIENT AUTHENTICATION

1.1. Strong client authentication (SCA) was established under Directive (EU) No. 2015/2366 on payment services in the internal market ("PSD2") and implemented by means of Delegated Regulation (EU) 2018/389 ("RTS"), and means authentication based on the use of two or more mutually independent elements from the categories of knowledge (what only the user knows), possession (what only the user holds) and inherence (what the user is), where the failure of one of them does not affect the reliability of the others, and the process is designed to protect the confidentiality of authentication data.

1.2. All card transactions carried out by a customer, whether point-of-sale or card-not-present (CNP) transactions, may only be initiated using Strong Customer Authentication (SCA) unless such card transaction falls outside the scope of PSD2 (Exemption from applicability - Article 2) or falls under one of the exemptions listed in PSD2 (Exclusions - Article 3).

1.3. The Merchant acknowledges that the application of an exemption or exclusion relating to strong client authentication (SCA) requires the prior written consent of Worldline NV/ SA (hereinafter referred to as "Worldline") and that such consent is granted by Worldline at its sole discretion.

2. EXCLUSIONS FROM STRONG CLIENT AUTHENTICATION

2.1. PSD2 sets forth the cases where Strong Customer Authentication does not apply to the Cardholder:

2.1.1. Mail/Phone Order (MPO):

2.1.2. transactions where the card details are transmitted by telephone or by mail.

2.2. Merchant Initiated Transactions (MIT): If a card payment transaction is initiated by or through a Merchant, Strong Customer Authentication (SCA) does not apply to the transaction provided that:

2.2.1. the Cardholder has first granted a mandate using Strong Customer Authentication (SCA), thereby authorising the Merchant to initiate a transaction or multiple transactions using the card,

2.2.2. the mandate is based on a contract between the Merchant and the Cardholder governing the provision of products or services

2.2.3. transactions initiated by the Merchant do not require any other specific action by the Cardholder to be preceded in order to be initiated by the Merchant.

3. EXEMPTION FROM STRONG CLIENT AUTHENTICATION

3.1. PSD2 allows for certain exemptions where the Cardholder does not have to undergo Strong Customer Authentication (SCA).

3.1.1. Exemption at the point of sale.

3.1.1.1. Contactless payments: contactless card transactions are excluded from Strong Customer Authentication (SCA) where:

- the value of a single card transaction does not exceed CZK 500,
- the aggregate value of payment transactions since the last application of Strong Customer Authentication (SCA) (by the Cardholder) does not exceed EUR 150.00; and
- the number of consecutive contactless card transactions since the last application of Strong Customer Authentication (SCA) (of the Cardholder) does not exceed five transactions.

3.1.1.2. Fares and parking: transactions made at a point of sale or at unattended payment terminals, specifically for the purpose of paying fares (e.g. tolls for the use of a toll road) or parking fees, are excluded from Strong Customer Authentication (SCA).

3.1.2. Exemption for Card-Not-Present transactions (CNP).

3.1.2.1. Low-value transactions: Worldline may waive the Strong Customer Authentication (SCA) obligation if:

- the value of the card transaction does not exceed EUR 30.00,
- the aggregate value of payment transactions since the last application of Strong Customer Authentication (SCA) (of the Cardholder) does not exceed EUR 100.00 and Strong Customer Authentication
- • the number of card transactions without the physical presence of the card (CNP) since the last application of Strong Customer Authentication (SCA) (of the Cardholder) does not exceed five transactions.

3.1.2.2. Recurring transactions: If Strong Customer Authentication (SCA) is applied to the first in a series of recurring card transactions of the same amount, then subsequent transactions within a period of up to 12 months after the application of Strong Customer Authentication (SCA) may be exempt from the requirement to apply Strong Customer Authentication (SCA) if all other authentication requirements are met and the identifiers of the original transaction are attached to subsequent card transactions.

3.1.2.3. Transaction risk analysis: The Service Provider may, at its discretion, allow the Merchant not to apply Strong Customer Authentication (SCA) for Card-not-present transactions (CNP). An assessment of the decision to grant such an exemption will be based on several criteria, such as the overall fraud rate and exemption limit (as set forth in the RTS Regulation and the card systems rules), the Merchant's transaction history, the Merchant's transaction patterns, the Merchant's business activities, the Merchant's geographic location, the Merchant's average customer, the Merchant's level of system security, the Merchant's solvency and financial liquidity, and the Merchant's overall financial standing. Even if the transaction risk analysis is successful, the Service Provider may reject the transaction based on a real-time analysis and risk assessment of the transaction. The Merchant understands that the transaction risk analysis exemption and the maximum transaction value for such exception depend on the Service Provider's overall fraud rate and exemption limit. The Merchant acknowledges that in the event that the total fraud rate of the Service Provider exceeds the limits set forth in the RTS Regulation or the card system rules, the Service Provider will no longer be able to offer this exemption at all or will only be able to offer this exemption in a limited manner. The Service Provider will use commercially reasonable efforts to inform the Merchant of such circumstances in advance.

3.1.2.4. Trusted payee: If the Merchant is designated as a trusted payee by the Cardholder, then the Service Provider may process transactions without applying Strong Customer Authentication (SCA) and must forward this information to the card issuer, who will assess whether the Merchant is listed as a trusted payee and whether it wishes to approve the transaction.

4. ELECTRONIC PAYMENT ECOSYSTEM

4.1. The Merchant acknowledges that even if a transaction falls within the parameters described in Articles 2 or 3, the transaction may be rejected by another entity in the payment chain (such as a card issuer). The Service Provider shall not be liable for any rejection by such third parties.

4.2. The Merchant will be responsible for properly performing Strong Customer Authentication (SCA) at both physical and virtual points of sale and must ensure that transactions sent to the Service Provider are correctly identified (e.g. the Merchant will not send a transaction as MIT or MPO if it is not consistent with reality, and the Merchant will not apply a parking fee exemption if the activity cannot be classified in this manner). The Service Provider has the right, but not the obligation, to verify compliance of individual transactions where an exemption or exclusion has been applied. Upon the Service Provider's first

request, and no later than 2 business days after such request, the Merchant must provide the Service Provider with all necessary documentation to justify the exemption or exclusion.

4.3. The Merchant acknowledges that the Service Provider may, at its sole discretion, revoke any Strong Client Authentication (SCA) exemption granted to the Merchant at any time.