IMPACTS OF EUROPEAN DIRECTIVE PSD2

Worldline

CONTENTS

01 Introduction

The purpose of this document is to highlight for merchants using Worldline payment services the implications of European Payment Service Directive (PSD2).

It contains an introduction to what the PSD2 directive is, then the specific implications for merchants offering over the counter payment services (in the store) or remotely (e-commerce). Against this background, changes to payment scheme rules caused by this new directive are considered and mentioned if relevant.

The document also sets out the measures which Worldline will ask merchants to take in order to be ready for the PSD2 directive and the new payment scheme rules (mandatory Strong Customer Authentication, and consequently 3D Secure), as well as a schedule.

02 The regulatory context

2.1 PSD2 and EBA RTS

Several elements of the payment services directives 2015/2366, known as PSD2, have an impact for merchants. One of the most important objectives of the new directive concerns protection of the paying customer through the three pillars: his information, his consent and his Strong Customer Authentication (mandatory in B2C).

The European Banking Authority (EBA) has defined certain requirements of the directive through Regulatory Technical Specifications (RTS), including those relating to Strong Customer Authentication (SCA) of the cardholder, which will apply from 14 September 2019.

2.2 Geographic coverage

The PSD2 directive is applied to all payment transactions within the European Economic Area (EEA), i.e. the European Union, including the United Kingdom (at least until Brexit), Norway, Liechtenstein and Iceland.

As regards Strong Customer Authentication of the cardholder (SCA), this applies when the acquirer and the issuer are located in the EEA. However, if one of them is located outside the EEA, it is no longer mandatory. For example, a merchant whose acquirer is Worldline Belgium must enable Strong Customer Authentication for a cardholder whose bank is located in France, but not necessarily for a buyer whose bank is located in the United States, in Switzerland or in China. In the special case of a cardholder whose bank is located in the United Kingdom, Strong Customer Authentication is mandatory at least until Brexit is applicable.

2.3 Obligations from mid-January 2018

New rules must be implemented from January 2018; they relate principally to information and the payer's consent.

Information for the payer
The payer must be informed of the conditions of his payment instrument. This relates, for example, to:

- the final period for making the payment (for example, in the case of payment on delivery),
- the reserved amount at the time of a reservation (for example, during check-in at an hotel or when buying petrol from an automatic fuel dispenser, where the final amount of the transaction is not known in advance),
- foreign exchange costs or exchange rates,
- or even additional charges (surcharging) or reductions linked to the use of a means of payment when this is authorised by the Government where the merchant has his business.

For transactions, if the information is not known by Worldline (for example, delivery date, foreign exchange costs when these are calculated by the merchant, surcharging) or if the payment page on the Internet is not presented by Worldline, it is for the merchant himself to inform the consumer (via his PSP if applicable).

Payer's consent
The payer must give explicit consent to each payment transaction or pre-authorisation in his presence. For an over-the-counter transaction in CHIP & PIN, consent is proved, for example, by entering the PIN. For an over-the-counter transaction in contactless mode, presentation close to the terminal after viewing the amount equates to the holder's consent.
In the case of a sale over the internet, this can be done by inviting the cardholder to approve the transaction data by clicking on a button.

2.4 The obligation to Strong Customer Authentication starting from September 2019

Strong Customer authentication of the cardholder (SCA) is intended to reduce fraud rates. It will be mandatory from 14 September 2019 when a cardholder initiates an electronic payment, for the exact amount of the payment, for the pre-authorised amount in case of a reservation, for the whole of a series of payments (knowing that in this case, any change to the conditions will need a new authentication).

What is Strong Customer Authentication?

Users will have to provide at least two separate elements out of these three:
- Something they know (a password or PIN code) -- knowledge
- Something they own (a card, a mobile phone) -- Possession
- Something they are (biometrics, e.g. fingerprint or iris scan) -- Inherence

Strong Customer Authentication applies both to over-the-counter payment and to remote payment. For example, on a payment terminal, inserting a chip card (something owned) and entering a PIN (something known) are considered as a Strong Customer Authentication method.

For remote payment, the use of a static password for an authentication to the holder's bank is not considered as being a Strong Customer Authentication. In contrast, the use of an equipment capable of generating a dynamic authentication code specific to each transaction or a smartphone coupled to facial recognition or a digital fingerprint is considered as a Strong Customer Authentication. It is expected that the banks will eventually roll out user-friendly methods of authentication by biometrics (for example, digital fingerprint, facial recognition) on the customer's smartphone, which would go some way to greater acceptance of these mechanisms by consumers.

PSD2 has also defined cases where Strong Customer Authentication of the cardholder does not apply:
- If the payer's bank (the issuer) or the payee's bank (the acquirer) is located outside the EEA,
- If the payment is initiated by the payee (for example: a direct debit)
- To paper payments (cheques, TIP)
- To (paper-based) mail order / telephone order
- If an exemption defined by the RTS SCA can be applied, for example if payment is made on vending machine / kiosk for transport (for example a motorway toll) or for parking.

It is important to note that exemptions can bypass Strong Customer Authentication, but are not an obligation.

Remember also that exemptions are not routine and that even if the conditions for exemption are met, the final decision rests with the issuer (the payer's bank) which may or may not grant it, depending on its own criteria (technical capacity to manage it, risk of fraud, arrangements agreed with the cardholder, etc.).

2.5 The role of payment schemes

Acquirers of transactions by payment card (e.g. Worldline) and payment card issuers must comply with:
- The law in force (e.g. PSD2)
- The rules defined by card payment schemes for which they offer services to their customers, who in principle must comply with the requirements of the legislators or regulators

For example, the RTS stipulates an exemption for contactless payment over-the-counter, with maximum amounts to be obeyed. A payment scheme may decide to impose more restrictive rules on its licence holders. Likewise, an issuer may also decide, for its own reasons, to implement more restrictive solutions; for example, in this case, lower ceilings than those imposed by the payment scheme, with these not allowed to exceed those set by the RTS. This may have the consequence that the merchant might observe patterns different from the cards of his customers (for example, this card accepted without a PIN for a contactless transaction of €45, whereas another card demands a PIN for the same amount).

2.6 The different exemptions from Strong Customer Authentication

2.6.1 Exemptions from Strong Customer Authentication for over-the-counter payments

The RTS stipulates 2 exemption options for over-the-counter payments, as well as those defined earlier:
- For low value contactless transactions;
- For transactions on a vending machine or terminals used for parking or transport.

The exemption for a contactless transaction can be invoked:
- If the amount of the transaction is less than €50;
- If, since the last transaction with Strong Customer Authentication by the cardholder, the maximum amount of contactless transactions, regardless of the merchant, or the number of contactless transactions has not exceeded a maximum (velocity criteria) defined by the RTS (max €150 or 5 transactions, at the issuer's discretion, which can also lower these ceilings).

Only the issuer can approve the velocity criteria. Therefore, on the payment terminal, a contactless transaction could be initiated without a request for entry of the PIN, but the issuer would have to refuse it or request that the PIN be entered on the terminal, depending on the result of the validation of the velocity or maximum amount criteria.

2.6.2 Exemptions from Strong Customer Authentication for remote payments

The RTS stipulates 5 exemption options for remote payments (e-commerce), as well as those defined earlier (§2.4):
- Trusted Beneficiaries or White-Listing
- Recurring transactions
- Low value transactions
- Corporate payments
- Transactional Risk Analysis

Trusted Beneficiary or White-Listing

White-Listing is the option for a cardholder to declare, to the issuer of his card, in general his bank, a merchant whom he trusts and for whom he does not wish to make a Strong Customer Authentication while executing remote transactions, provided the latter meets the security criteria set by the bank.

International payment schemes recommend to card issuers (the banks) to stimulate, during the phase of authentication of the cardholder to his bank while executing a 3D Secure transaction, adding a box to be checked in which the payer can ask for the merchant to be included in his list of Trusted Beneficiaries (the white list).
Payment schemes anticipate that the merchant could be informed, in response to the execution of the transaction, that he is in the consumer's white list.

The regulations also stipulate that the cardholder could, at any moment, withdraw a merchant from his list of Trusted Beneficiaries, which will be facilitated by the bank through online mechanisms.

Exemption for a Trusted Beneficiary (White List) is certainly the simplest method for a merchant to benefit from exemption from Strong Customer Authentication. However, this relies on:

- The trust afforded by consumers to the merchant,
- Information of the payer by the merchant to encourage it to register in the white list,
- The capability of the bank to manage white lists and ease of registration,
- And on the consumer's bank (the card issuer) which decides to grant or refuse exemption for each transaction.

Recurring transactions
An exemption from Strong Customer Authentication is applied for a series of remote transactions for the same amount to a single beneficiary when the payer has given his consent for them. However, Strong Customer Authentication is required for the first transaction (the contract) or for each modification of the series conditions.

Low value payments
An exemption from Strong Customer Authentication for a low value remote payment can be invoked:

- If the amount of the transaction is less than €30;
- If, since the last transaction with Strong Customer Authentication of the holder, the maximum amount of low value remote transactions, regardless of the merchant, or the number of low value remote transactions does not exceed a ceiling (velocity criteria) defined by the RTS SCA (max €100 or 5 transactions, at the issuer's discretion, which can also lower these ceilings).

Only the issuer can approve the velocity criteria. Consequently, it is recommended that the transaction be executed in a manner that will enable the issuer to decide whether he can or cannot apply the exemption and, if this is not the case, then to initiate a Strong Customer Authentication session with the cardholder.

"Secure Corporate" payments
Exemptions are also valid for payments initiated by businesses with a debit from the business account (for example, central settlement cards, centralised accounts and (closed-loop) virtual cards). In contrast, corporate cards (with debit from the employee's bank account under special conditions) are similar to B2C transactions and are not covered by these special exemptions.

Exemption for transactional risk analysis (TRA)
The exemption from Strong Customer Authentication for a remote transaction referred to as 'risk analysis' can be invoked by the acquirer (on behalf of the merchant) and by the issuer if the following two conditions are met:

1. That the transaction is declared safe (for example, no infection of the user's workstation by a malware, no abnormal disbursements by the payer, location of the payer, transactions history, etc.)
2. That the fraud rate for remote transactions when compared to the total volume of sales transactions (for both the Issuer and Acquirer, but not for a merchant or his PSP/Gateway) is below preset ceilings:
   - 0.13% if the amount of the transaction is less than 100 euros
   - 0.06% if the amount of the transaction is less than 250 euros
   - 0.01% if the amount of the transaction is less than 500 euros
   - Exemption not applicable for transactions of over 500 euros.

As will become clear later, it is recommended that the transaction be initiated in 3D Secure mode, in order for the merchant to indicate that he wishes to benefit from this exemption, or for the issuer to apply the exemption itself if it meets the conditions and is judged appropriate for its customer, the cardholder.

03 Consideration of PSD2 by payment schemes

Characteristics of 3D Secure 2.0

International payment schemes have defined, within EMVco, their standardisation body, a major upgrade of the 3D Secure specification, referred to as 3DS 2.0, used for remote payment. The principal aim of 3DS 2.0 is to reduce payment fraud, at the same time strongly improving user-friendliness for the cardholder, in particular by providing the issuer with more information on the context of the transaction, in order to allow the latter to decide whether it should or should not proceed with strong authentication of the cardholder, or even by standardising the card holder authentication process through his smartphone.

This new version primarily brings the following advantages:

- The logic of data exchange between the PSP of the merchant and the issuer is adapted and enriched in order to provide the issuer with a greater amount of contextual data relating to the transaction in progress, so as to enable it to refine its risk assessment and consequently to decide whether it cannot proceed with a Strong Customer Authentication of the cardholder, provided he meets the exemption conditions.
- Integration in mobile apps enabling a more user-friendly experience from his smartphone. Thus, optimised integration of 3D-Secure in an app may enable:
  - Initiation of 'authentication through the app (embedded mode): in other words, that the merchant's 3D-Secure component and the app dialogue directly with the means of authentication, with no need for the payer to be redirected to the issuer's website (for example, for an in-app purchase, the app could trigger a verification of the digital fingerprint, in lieu of 3D-Secure authentication, provided that the issuer allows this)
  - Initiation via a redirection to a banking application installed on the smartphone, and no longer via a redirection to a web page; where, from the banking app, via a confidential code or a biometric authentication, the 3D process would be implemented – provided that the issuer allows this.
- A possible authentication via a channel different from that of the purchase instrument (out-of-band or decoupled mode). In the case of purchases on a gaming console, on a smartspeaker, or even for a telephone sale, 3D-Secure 2.0 will trigger authentication via another channel (for example, on the smartphone's bank application, woken up via an alert). With thoroughness, an in-app purchase on smartphone can be the subject of an out-of-band authentication on the same smartphone, which would return to a redirection on to the banking app. It can also be contemplated that a purchase over conventional internet from his PC, might be the subject of an out-of-band authentication on smartphone, without redirection from the payer's browser to the payer's bank. Of course, provided that the issuer implements this authentication and that the payer is equipped.

Deployment of 3D Secure 2.0 and coexistence with 3D Secure 1.0

Deployment of 3D Secure 2.0 is required by the Visa and Mastercard after April 2019.
However, as will become clear below, it is recommended that the merchant's PSP supports both 3DS 1.0 and 3D 2.0 until withdrawal from service of 3DS 1.0, currently planned at the end of 2020 for Visa and Mastercard.

Regarding other card payment schemes:

- Cartes Bancaires: 3DS 2.0 will be launched during 2019 with progressive migration
- Bancontact: 3DS 1.0 is already mandatory, migration to 3DS 2.0 will take place shortly (schedule to be confirmed)
- American Express: it is necessary to integrate 3D-Secure 1.0, then to add 3D-Secure 2.0 to it.
- Diners: 3D-Secure 1.0 integration is recommended, according to the origin of the holders
- JCB, UnionPay, Diners/Discover Network: the extra-European origin of the cards issued allows an exemption from Strong Customer Authentication
- For other private solutions: see with them the possible impacts of the PSD2 directive on their payment services.

New rules for transfer of liability

The rules for transfer of liability between issuer and acquirer in case of disputes will change with the introduction of PSD2 and the new version of 3D Secure, as well as the merchant's ability to demand an exemption from Strong Customer Authentication in the first message exchanged between him (or the technical acceptance service providers, commonly referred to as PSP or Gateway) and the issuer. The rules may differ slightly between schemes.

If the merchant allows the issuer to make a Strong Customer Authentication, the merchant is released from his liability, and the issuer proceeds or does not proceed with a Strong Customer Authentication of the cardholder, according to the type of exemption that he can invoke (e.g. White Listing, issuer side TRA, low value transaction).

If the merchant deliberately does not allow the issuer to carry out a Strong Customer Authentication (for example, by failing to initiate the transaction in 3D Secure mode), the merchant will bear the risk of fraud.

Furthermore, if the merchant initiates a transaction in 3D Secure mode and requests its acquirer the exemption from Strong Customer Authentication for risk analysis (TRA) and if the issuer accepts this demand without forcing a Strong Customer Authentication of the holder, the acquirer will be responsible in case of fraud and will transfer the cost to merchant.

For example, during a transaction initiated in 3D-Secure 2.0, the issuer will be able to decide not to do a Strong Customer Authentication with the consumer, if it can invoke one of the exemptions (white listing, issuer side TRA, low value transaction). In these cases, the issuer is responsible.

As soon as the rules for the schemes are finalised, additional information will be shared.

04 Aspects to be considered by merchants

The obligations of information for the consumer and obtaining his consent have been applicable since January 2018.

The obligations for Strong Customer Authentication of the cardholder must be implemented on September 14th 2019.

4.1 Over-the-counter payments

As explained previously, two cases of exemption have been stipulated for over-the-counter payment, viz. low value contactless transactions and transactions for transport and parking on an unattended machine. In all other cases, a Strong Customer Authentication of the cardholder must be executed.

A terminal accepting contactless transactions could therefore not be equipped with a PIN pad.
However, it is recommended to deploy terminals with a PIN pad in order to also support transactions in contact mode. Thus, in the case the Issuer might invoke Strong Customer Authentication for a contact-less transaction if the thresholds (amount or number-based) are reached, the payment will be done.

A transport or parking services operator will be able to decide to install unattended payment terminals without PIN pad (and therefore not allowing entry of a PIN). However, as exemption is an option, it could be only in certain cases that the issuer desires a Strong Customer Authentication. Currently, it appears reasonable to foresee a terminal without PIN pad on a motorway toll or on a street parking meter; however, on a private parking machine, it could be useful to foresee a terminal with PIN pad.

4.2 Remote payments

As explained previously, five cases of exemption from Strong Customer Authentication are stipulated in the remote payments context: Trusted Beneficiaries or White-Listing, recurring transactions, low value transactions, corporate payments and Transactional Risk Analysis. In all other cases, a Strong Customer Authentication of the cardholder must be executed.

As was also explained above, payment schemes are imposing the roll-out of 3DS 2.0 as a technical solution in the remote transactions context. They consider that this will reduce fraud significantly, while having no impact on the conversion rate, as the 3DS 2.0 solution must allow the issuer not to carry out a Strong Customer Authentication of the cardholder as a matter of routine.

During the 3DS 2.0 roll-out period, it is strongly recommended that the merchant's PSP supports both 3DS 1.0 and 3DS 2.0, in order to profit from the transfer of liability regardless of the solution supported by the issuer during the transition period.

In summary, as a merchant offering remote payments, ensure that your PSP has activated 3DS 1.0 and, if possible, 3DS 2.0 operational before 14 September 2019, unless there is a valid exemption. Merchants who have not yet implemented 3D Secure must consider reviewing the consumer's purchasing experience and ensure that Strong Customer Authentication is integrated correctly into the sale process.

Merchants can also foresee calling on the exemptions from Strong Customer Authentication authorised by PSD2. As will become clear later on, in the majority of cases, this happens nonetheless by initiating the transaction in 3D Secure mode.

Merchants who currently do not use 3D Secure for all transactions as a matter of routine (for example: activation of 3D Secure for high value risk sales or if the holder is located in a country at risk, but not for other transactions); [for them], this method of operating will have to be reviewed in light of the obligation to Strong Customer authentication and the cases of exemption authorised (see above).

Exemption for Trusted Beneficiary or White-Listing
The decision to use exemption is made by the issuer (and not by the merchant, his PSP or the acquirer). The merchant can encourage the consumer to include him in the list of Trusted Beneficiaries.

The transaction must be initiated in 3D Secure mode. If the issuer supports this exemption mode, it will be able to apply it if the merchant is already in the list of beneficiaries. If this is not the case, a Strong Customer Authentication is required. (It is stipulated that issuers allow registration in the white list during the Strong Customer Authentication associated with a transaction.)

Exemption for recurring transactions
The first transaction (the contract) must be made with Strong Customer Authentication (in 3D Secure).
The following transactions may be exempt Strong Customer Authentication without using 3D Secure, in which case certain issuers may refuse it, despite everything.
In order to link the subsequent transactions to the previous SCA transactions specific reference codes must be incorporated in the data exchange.

Exemption for low value transaction
The decision to use exemption is made by the issuer (on the basis of the amount of the transaction, velocity conditions and the issuer's strategy towards its cardholder customer).

The transaction must be initiated in 3D Secure mode and the issuer will decide whether or not to proceed with Strong

Customer Authentication of the cardholder.

Exemption for Transactional Risk Analysis

The transaction must be initiated in 3D Secure mode. A flag must be set to inform the issuer that the merchant wishes to benefit from this exemption. If the issuer agrees to the merchant's request, without proceeding with Strong Customer Authentication of the cardholder, the acquirer becomes responsible in a case of fraud and transfers the cost to the merchant.

This exemption can also be applied by the issuer of the payment card without a request from the merchant. In this case, the issuer becomes responsible in a case of fraud.

To benefit from it, merchant must perform a proper risk analysis (criteria provided by EBA) to establish that the transaction is indeed low risk.

05 Examples of implementation of special transactions

Wallets

In the case of third party wallets having an authentication agreement delegated by the issuer (example, Paylib for Cartes Bancaires, mobile Bancontact), the Strong Customer Authentication is handled by the provider of this wallet (as delegated by the issuer), with the option to invoke exemptions from Strong Customer Authentication as well.

In the case of a merchant wallet (storage of identifiers on the merchant's site) or third party wallets not having a delegated authentication agreement from the issuer, the payment transaction will be subject to 3D Secure Strong Customer Authentication, as with any transaction made with a card not stored in a merchant wallet, at the same time being eligible for the exemption rules.

Apple Pay, Samsung Pay

These means of payment, made available on the cardholder's smartphone and coupled with a Strong Customer Authentication method of the biometric type, recognised by the issuer of the payment card, can be used indifferently in an over-the-counter context, in contactless mode and for remote payments if they are integrated in an e-commerce site.

Do not fail to integrate these means of payment, which are used in card transactions (Visa, Mastercard, American Express, Cartes Bancaires) and are possible with your acquirer, Worldline. Manufacturers of mobile terminals have seen an opportunity here and will be launching matching communication operations.

Examples of remote transactions and processing recommendations

Below are listed transactions commonly performed by merchants.
It should be noted that the schemes will adapt their protocols for processing particular types of transactions. Not everything is totally defined yet.

A few general rules are set out below. Exemptions which merchants may try to invoke are also applicable to these rules.

Unitary payment – Single standard payment

Example: I purchase a product on a website. Product is immediately available for delivery today. Payment is executed today.
Payment initiated by: Payer.
Behaviour: Strong Customer Authentication, with possible exemption.

Deferred payment (with amount less than or equal to the initial amount; for which the amount is not known in advance)

Example: I purchase several products on a website. Products aren't immediately available for delivery today. I agree to pay today but the merchant will process the payment only when sending the products to me. If one of the products can't be sent, the amount that will be debited, will be lower than the amount for which I gave my consent.

Payment initiated by: Payer
Behaviour: Strong Customer Authentication (with possible exemption) for the global amount (or if the amount isn't known in advance, for the maximum possible amount), clearing (with reauthorization or not) for the exact amount.

Split payments - payments on instalment, subscriptions without renewals by the silence procedure

Example: If a sale is covered by more than one delivery, and transactions with each shipment, the user having consented to the transaction in its entirety.
Other example: payment is split in 3 transactions executed each month for a 3 month period
Other example: subscription to a magazine for a period less than one year.

Payment initiated by: Payer
Behaviour: Strong Customer Authentication for the global amount when the payer is in session. Several clearings when product delivered (reference to initial authorization, with or without reauthorization, depending on Scheme rules). In the case of small amounts, the merchant may also try to invoke the low value exemption with each payment.

Series of fixed amount payments

Example: "online music", "video on demand" subscription
Payment initiated by the Payer for the 1st transaction and by the merchant for the following transactions
Behaviour: SCA for the 1st transaction, not for the following ones. If a product or a service is sold with the first transaction (e.g. set-up costs), then the SCA must include the total amount of the transaction. In the case of small amounts, the merchant may also try to invoke the low value exemption with each payment.

1-click payments

Example: 1-click payment from a merchant application or a merchant wallet and for which the consumer has been authenticated by the merchant.
Initiated by: Payer or merchant (depending on the several transactions cases described above)

Behaviour: complete knowledge of the customer by the merchant does not change the rules set out above in any way and Strong Customer Authentication is applied according to case. Thus, the purchase of a book from an online library is a transaction initiated by the payer and must be covered by a Strong Customer Authentication or an exemption. However, from his pre-registration in the wallet, the merchant can request the issuer to be added to the White-list of Trusted Beneficiaries.
The customer's registration (or renewal) in the wallet is also among the cases included in the scope of Strong Customer Authentication.

Transactions initiated by merchants

A further clarification from the European Banking Authority must specify and confirm the concept of Merchant Initiated Transactions, which will (or will not) lift the uncertainties surrounding the conditions for processing certain specific transactions.

Transactions initiated by the payer or by the merchant

According to the RTS (technical specifications associated with PSD2), only operations initiated by the payer fall within the scope: "Any payment operation or any series of payment operations covered by an ad hoc consent by the customer for a given maximum overall amount".
On this basis, certain payment schemes assume that operations initiated by the merchant must not be the subject of Strong Customer Authentication.

Inter alia, this relates to purchases of goods and services for which the amount can neither be determined, nor estimated by the merchant, where transactions agreed by the payer cannot be collected. In contrast, the initial mandate or changes related to the conditions of payment should be the subject of Strong Customer Authentication

The EBA has not yet confirmed that card transactions initiated by merchants, without intervention by the payer, are outside the scope of Strong Customer Authentication.

One example: bill payment

Example: payment of an electricity bill the amount of which varies according to consumption.
Initiated by: Merchant
Behaviour: 1st transaction with SCA, following ones without SCA. Some schemes invite merchants to do the 1st SCA at the maximum amount that could be reached in the following transactions.

Special cases

There is a complete range of special cases based on very specific use cases.
Some examples:

- Ride-share services, for which the fare is not known in advance,
- the hotel business, where additional sums may be paid (breakfast), after payment for the room, leasing, or charges may be made for cleaning, filling with petrol, or the application of excesses,
- the hotel business or leasing, where the customer cannot pass the counter to pay his final invoice (for example, outside opening hours),
- multi-merchant baskets, in the case of market places or travel agencies, and capable of triggering multiple transactions, directly by the end users,
- cases of price increases (if the delivery conditions have changed, if one product has been replaced by another with the customer's agreement),
- a no-show when a customer who has ordered a service fails to appear or is unable to receive this service.

Merchants can complete these transactions in different ways:

- by relying on the concept of transactions initiated by the merchant, if these are accepted by the EBA,
- by performing a Strong Customer Authentication, using decoupled or out-of-band mechanisms,
- by performing a first authentication for an amount clearly well above the maximum possible amount,
- by recommending very strongly to the consumer that he register the merchant in the list of Trusted Beneficiaries.

06 Summary of actions

1. Integrate 3D-Secure 1.0 on your website before 14 September 2019, with your technical acceptance service provider: necessary to be in compliance and ensure that you do not lose any transactions. Ensure also that you are registered correctly with your acquirer, Worldline.
2. Migrate to 3D-Secure 2.0 during 2019 to benefit from exemptions and improved integration with your mobile site, while keeping 3D-Secure 1.0 to handle cases of issuers not yet ready on 3D-Secure 2.0.
3. Ask your acquirer, Worldline, to be registered in the 3D-Secure 2.0 programme (even if you are already in the 3D-Secure 1.0 programme)
4. In the case where you initiate a 3D-Secure 2.0 transaction and the issuer does not support this version, ensure you are able to implement authentication in 3D-Secure 1.0
5. Improve the Issuer's risk analysis to benefit more easily from an exemption, by sharing holder data (mail, billing and delivery addresses, telephone, etc.) via your PSP and 3D-Secure 2.0.
6. Do not forget to include the 3D-Secure logos for the different schemes on your Web pages. Please note that Mastercard has a new logo (Mastercard Identity Check).
7. Rethink the purchasing and payment experience based on these new authentication obligations, more particularly for mobile sales.
8. Have a simple name, unique and which identifies you correctly in order to optimise your recognition by holders in white lists
9. For recurring payments a Strong Customer Authentication is necessary for the first. For subsequent payments, refer to the first authentication, so that the cardholder is not asked to re-authenticate himself
10. In the case of recurring payments with variable amounts, or if the final amount is not known in advance, for which you authenticate the holder for an amount higher than the transaction(s), inform and reassure your consumer
11. Do not forget to carry out a strong authentication, even for a transaction initiated by the merchant at a later date.
12. The authenticated amount must always be greater than or equal to the amount of the authorisation or the sum of the authorisations in the case of split payments.

07 Glossary

European Banking Authority (EBA)
Created in 2010, European financial system supervision authority.

PSD2
The European Directive (2015/2366/EU) on Payment Services, version 2

Fractioned payment (split payment)
Payment transaction covered by a number of operations to debit the consumer, based on successive deliveries of purchased goods.

Regulatory Technical Standards (RTS)
Regulatory technical standards published by the European Banking Authority and associated with PSD2.

SCA
Strong customer authentication