Elavon

PSD2 Practical Impact Guide

For face to face (card present)

September 2019

elavon.co.uk | elavon.ie

Contents

Introduction 3

Strong Customer Authentication 3

Authentication Factors 3

Chip and PIN transactions 4

Contactless transactions 4

Manually Processed transactions – cardholder present 4

Manually Processed transactions – cardholder NOT present 4

Exemptions from Strong Customer Authentication 5

- Unattended Card Acceptance Devices 5
- Out of Scope - ‘One Leg Out’ 5

Preparing for the deadline 5

What this means for your business 6

What to do if a transaction is declined 6

Don’t risk losing transactions, or losing customers 6

Introduction

The Payment Services Directive 2 (PSD2) requires Strong Customer Authentication (SCA) to be applied to all card transactions carried out in a face to face (card present) or in-store environment.

Aimed at reducing payment fraud and improving security for consumers and businesses across the European Union, this industry-wide change is being introduced by law on 14th September 2019.

Strong customer authentication

Strong Customer Authentication means that banks must authenticate the cardholder as being the genuine owner of the payment card before they approve the transaction.

To prove that they are the genuine owner of the card, cardholders will need to provide at least two out of three possible authentication factors to their bank when requested.

Authentication factors

These can include any combination of two of the following:

1 **Knowledge** – this refers to something only the cardholder and their bank knows. PIN is already the industry standard method used to satisfy this requirement.

2 **Possession** – this is something the cardholder has which is recognised by their bank. In the in-store environment, Chip and PIN and contactless acceptance devices automatically satisfy this requirement.

3 **Inherence** – this is something unique to the cardholder and verifiable by their bank. A fingerprint, facial recognition or an iris scan are examples of factors that will increase in use and availability over time as the technology evolves and matures.

Chip and PIN transactions

Chip and PIN is a well-established, proven and successful feature of the European payments landscape. These transaction types already satisfy the two-factor requirement and are compliant with the directive. Continue processing these transactions in the same way as you do today.

Contactless transactions

The convenience of contactless 'tap and go' transactions will continue, however the new regulations place upper limits on the amount of taps or cumulative transaction amounts that can occur before the cardholder's bank is required to challenge and authenticate the cardholder.

Cardholders can continue to make contactless purchases under €50 until they make either 5 consecutive contactless transactions without providing authentication or the total value of unauthenticated transactions exceeds €150. These are the upper limits set by the regulators. Banks can choose to implement stricter controls if they consider the transaction a high risk or your national regulator might enforce lower limits.

Either way, like today, you cannot predict when these limits are being reached or which particular transaction will trigger the 'step up' in security.

If you accept a lot of contactless transactions through your business already, you're probably familiar with this process. This is where the contactless tap is declined and the cardholder is prompted to enter their PIN or insert their card into the card reader to perform a Chip and PIN transaction.

This completes the transaction and resets the cardholders limit counters restoring their 'tap and go' capability.

Manually processed transactions – cardholder present

Manually processed transactions where the cardholder is present will no longer be permitted under the regulations. These transaction types include magnetic stripe and Chip and PIN 'fall back' transactions that are completed by manually entering the card details into your payment device. By law, these transaction types will now have to be declined by the banks because they cannot be authenticated with two factors.

Manually processed transactions – cardholder NOT present

If you manually key enter transactions into your payment device because you are taking telephone or mail order payments as part of your business, you can continue doing this. MOTO (Mail Order/Telephone Order) transactions are beyond the scope of the regulations.

Exemptions from Strong Customer Authentication

Unattended card acceptance devices

For practical reasons the regulations do not apply to certain industry types. These exemptions only apply to unattended transport and parking acceptance devices associated with the Merchant Category Codes (MCC) for that industry. All other unattended devices including vending machines are within scope of the regulations and must support the ability to perform SCA when requested via PIN, or Chip and PIN.

Out of scope - 'One Leg Out'

The law only applies to the European Economic Area (EEA)so cards issued outside of the region can still be processed within the EEA as usual, including magnetic stripe and signature, Chip and PIN 'fall back' and manually key entered transaction types. You cannot easily identify that a card was issued by a bank outside of the EEA. Continue to process your transactions as you do today and the cardholders' bank will automatically detect that these transactions do not need to be challenged.

Preparing for the deadline

The biggest changes introduced by the new regulations are being experienced in the higher risk transaction channels. These are payment transactions made over remote channels like the internet and mobile phones where the cardholder is not present and Strong Customer Authentication is not already in widespread use.

The unavailability of suitably evolved technology platforms required to make those changes has challenged the industry and prompted the European Banking Authority to consider an extension to the enforcement deadline.

Some national regulators have already committed to an extended compliance timeline for these more complex transaction flows in the 'virtual' environment so immediate enforcement is not to be expected.

This is not the case for your physical world transactions. Are you prepared?

What this means for your business

Continue to process your card transactions at the point of sale on your devices as you do today. The Chip and PIN processing experience will continue unchanged.

Be aware that for contactless transactions, you might see an increase in the number of times your customer is asked to enter their PIN or complete the transaction by inserting their card into the reader and performing a Chip and PIN transaction.

Your customers' payment experience might vary in the early months of the switch on and transition to the new 'step up' responses that banks will introduce. Some banks will need to go through a phase of card re-issuance to make the changes and not all payment accepting devices and their connecting gateways and processors are expected to be able to precisely co-ordinate their updates across the EU.

If your business is driven by high volumes of contactless transactions and you actively manage queues and busy checkouts, it is advisable to have more staff available in case of an uplift in PIN or Chip and PIN requests, but for the most part, you just need to ensure that your staff are briefed on the change.

What to do if a transaction is declined

Process your card and contactless transactions in the usual way.

If a contactless transaction does not appear to work or the transaction is declined, advise the customer to insert their card and perform a Chip and PIN transaction.

Provided that the cardholder has funds available, this procedure will reset their tap limit counters set by their bank and the transaction will proceed.

If the transaction is still declined, advise the cardholder to contact their bank and request another payment method in that instance.

Don't risk losing transactions, or losing customers

Ensure that all of your staff are aware of these changes. Increasing the levels of security on transactions helps all of us to be protected

Speak to your Customer Services Team for more details.

We make it possible. **You make it happen.**

UK **0345 850 0195** IRE **0818 202 120** **elavon.co.uk** | **elavon.ie**

Y3558V10919