Strong Customer Authentication:

Marketing Communications guidebook for Merchants

September 2019

Disclaimer

This presentation is furnished to you solely in your capacity as a customer of Visa and[/or] a participant in the Visa payments system. By accepting this presentation, you acknowledge that the information contained herein (the “Information”) is confidential and subject to the confidentiality restrictions contained in Visa’s Rules and[/or] other confidentiality agreements, which limit your use of the Information.

You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa or as a participant in the Visa payments system. The Information may only be disseminated within your organisation on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non-public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non-public information would constitute a violation of applicable U.S. federal securities laws.

Case studies, comparisons, statistics, research and recommendations are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice.

The products and services described in this document may be subject to further development and launch dates for specific features are indicative only. Visa reserves the right to revise this document accordingly.

As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This document represents Visa’s evolving thinking, but it should not be taken as a definitive position or considered as legal advice, and it is subject to change in light of competent authorities’ guidance and clarifications. Visa reserves the right to revise this document pending further regulatory developments. We encourage clients to contact Visa if they experience challenges due to conflicting guidance from local regulators. Where it makes sense, Visa will proactively engage with regulators to try and resolve such issues.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers are responsible for their own compliance with SCA requirements, and are encouraged to seek the advice of a competent professional where such advice is required.

Hello

We’ve created this guidebook to help your business prepare for the Europe-wide rollout of Strong Customer Authentication (SCA).

SCA will benefit everyone who makes and accepts Visa payments. It will mean a reduced risk of fraud and improved security. This will be good for businesses (like yours) and good for customers.

This guidebook contains advice and communications to help your business and staff prepare for the changes and why it is important to contact your Payment Service Provider (PSP).
It also contains materials to help you raise awareness of the changes on your website and in-store to customers.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Contents

Understanding SCA

SCA Customer experience

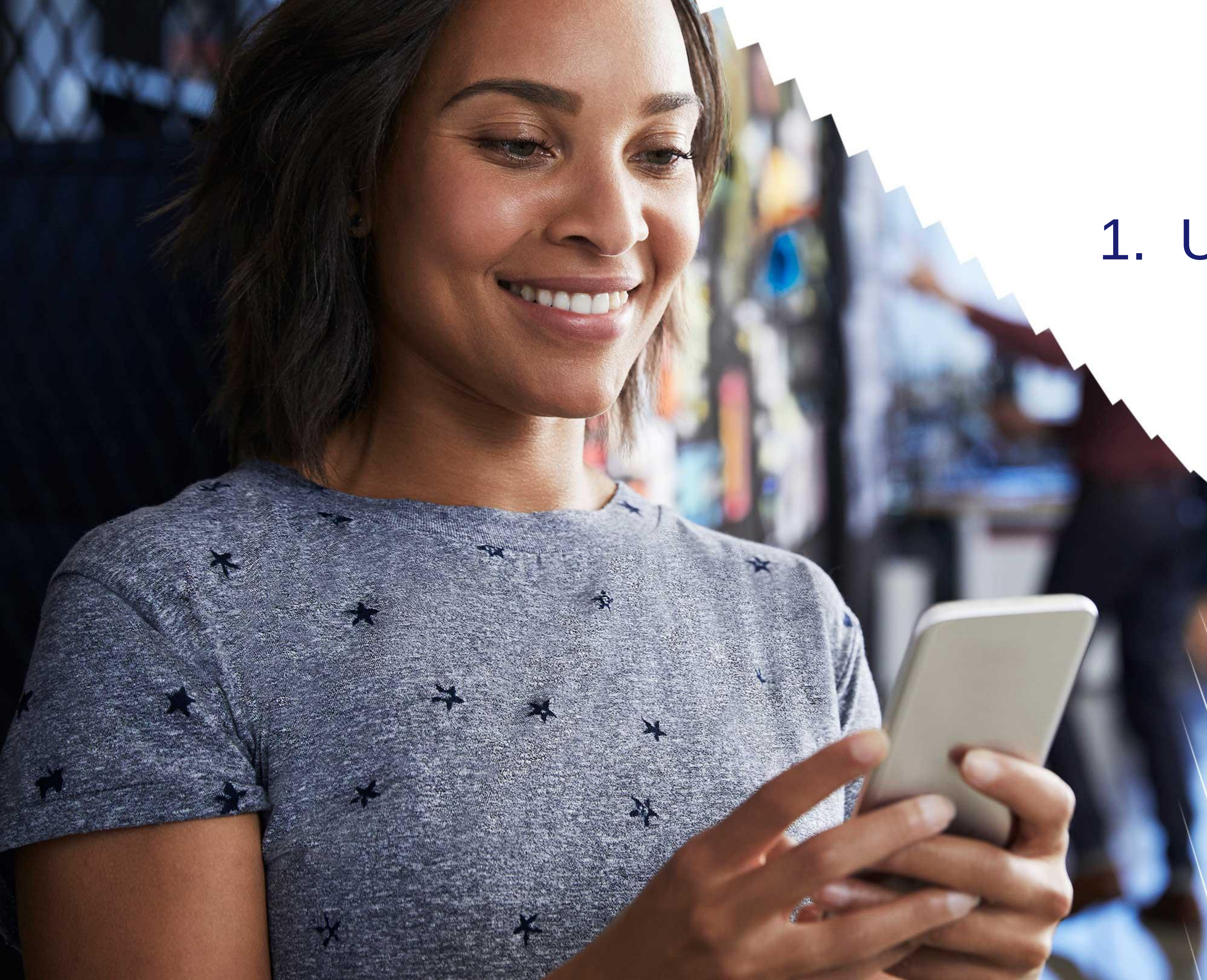
Implementing SCA

How to communicate to customers

Appendix:

Detailed Communications Material

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.



1. Understanding SCA

1.1 SCA in a nutshell

The European Union is introducing new security measures called Strong Customer Authentication (SCA), which may change the way customers pay online and offline/in-store making a contactless payment with their Visa.

It will affect all businesses based or serving customers in the European Economic Area (EEA) which accept credit or debit card payments.

These laws introduce security measures called two-factor authentication to help keep customers even safer when making payments transactions including those made online and via contactless. This is an industry-wide change.

As part of the changes, banks will receive more data to make informed decisions about whether two-factor authentication is needed.
Visa's SCA solutions use the latest technology, which analyses risk faster to create a more frictionless payment experience.

The increased levels of security and control will directly benefit customers by increasing their trust and confidence while shopping online or in-store.

Visa is working closely with participating Issuers and your PSP to help protect customers against unauthorised use of their card when they shop online or offline.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

1.2 Two-factor authentication

Following the implementation of SCA, your customers may have to confirm who they are by taking an additional security step when paying with their Visa. This is called **two-factor authentication,** which means they may have to provide information from at least two of the three categories below. What they will have to provide will depend on their bank’s requirements.

Something you know

such as a password or PIN

Something you have

such as a mobile phone, card reader or other device

Something you are

such as iris scans, facial recognition or a fingerprint

Your PSP can tell you what you need to do get ready, and about the implementation timelines. These are currently being considered by some local regulators. Your PSP may also have information on the changes on their website.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

1.3 The potential impact of SCA for your business

SCA will offer an opportunity to you and your customers by making payments even safer and offering even more protection against the risk of fraud.

If your business is prepared for SCA, you can offer your customers a quick and easy Visa payment experience and ensure you benefit from the upcoming improvements.

What SCA could mean for your business:

Customer authentication is coming – According to Visa's UK Issuer steering group, Issuers expect to request customer authentication on more transactions.[1]

Be prepared for SCA – A recent research study found that only 15% of businesses feel 'extremely prepared' for SCA, and only 40% expect to be prepared by September 2019.[2]

Keep your customer experience seamless to keep them coming back – 52% of customers who abandon their carts will purchase from alternative businesses with better payment flows.[3]

Contact your PSP to discuss the improvements that need to be made to build the new authentication process into your Visa payment journey. This will ensure your continued business success and help you stand out from your competitors.

[1] Visa UK Authentication Steering Group; Feb 19.
[2] The impact of SCA, 451 Research; May 19.
[3] The impact of SCA, 451 Research; May 19.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

1.4 What you need to consider about SCA

Keep your business moving – To continue to accept online and contactless Visa payments quickly and easily once SCA has been introduced.

You and your PSP can discuss any improvements such as enrolling for 3DS, making the most of the exemptions or upgrading your Point-of-Sale terminal. By doing so, you can optimise your customers' payment experience and make the most of the opportunities SCA offers.

Visa's commitment to improving awareness of SCA – To help you speak to your staff about the upcoming SCA improvements and their benefits, we've attached various communications in this guidebook.

A seamless customer experience – By understanding SCA you can ensure your customers receive a smooth payment journey and continue to shop with you.

To make sure your business is ready for SCA, contact your PSP today.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

2. SCA Customer experience

2.1 What SCA will mean for your customers

Once SCA has come into force, your business and customers will benefit from increased levels of security and a reduced risk of fraud.

SCA aims to help Merchants with enhanced transaction security and improve the customer experience with a greater number of completed sales. For customers, it aims to provide peace of mind through increased fraud protection and frictionless checkouts.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

2.2 Customer experience online

Online

Here's how your customers will make Visa payments when SCA is required.

Customers may need to confirm who they are when making a payment using their bank's chosen authentication method. They will do this by providing information from at least two of the three categories below (two-factor authentication):

Something they know – such as a password or PIN

Something they have – such as a mobile phone, card reader or other device

Something they are – such as iris scans, facial recognition or a fingerprint

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

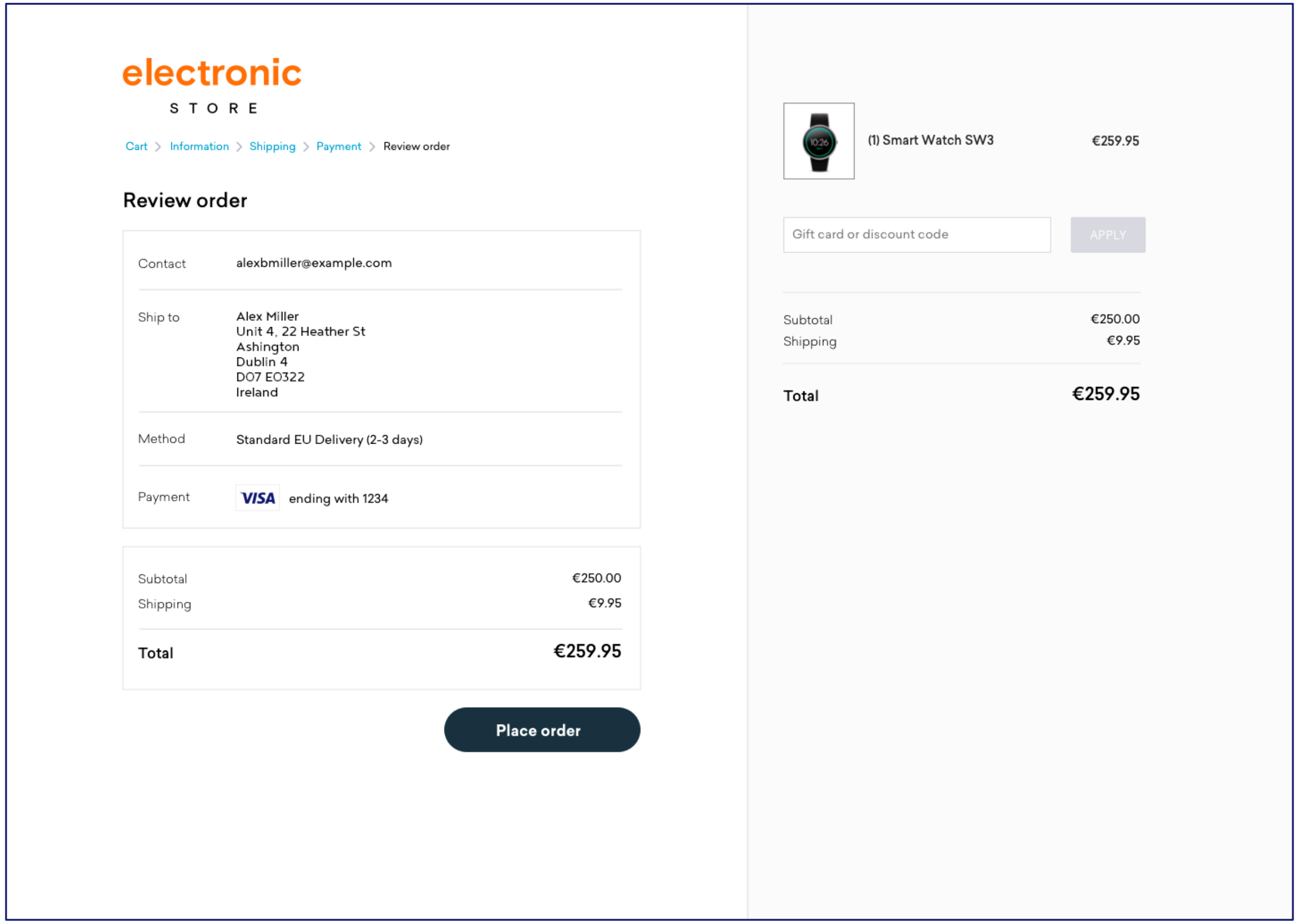
2.2 Customer experience online

Here's how your customers will make Visa payments once SCA is live:

Step 1.

A customer wants to make an online purchase using their desktop, laptop, mobile phone, or other digital device and goes to the retailer's checkout page.

Tip:
If a customer contacts you about issues regarding authentication, refer them to their Issuer for more information.



electronic STORE

Cart > Information > Shipping > Payment > Review order

Review order

Contact	alexbmiller@example.com
Ship to	Alex Miller Unit 4, 22 Heather St Ashington Dublin 4 D07 E0322 Ireland
Method	Standard EU Delivery (2-3 days)
Payment	VISA ending with 1234

Subtotal	€250.00
Shipping	€9.95
Total	€259.95

(1) Smart Watch SW3	€259.95

Subtotal	€250.00
Shipping	€9.95
Total	€259.95

Electronic store is an example Merchant created to demonstrate the purchase process only.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

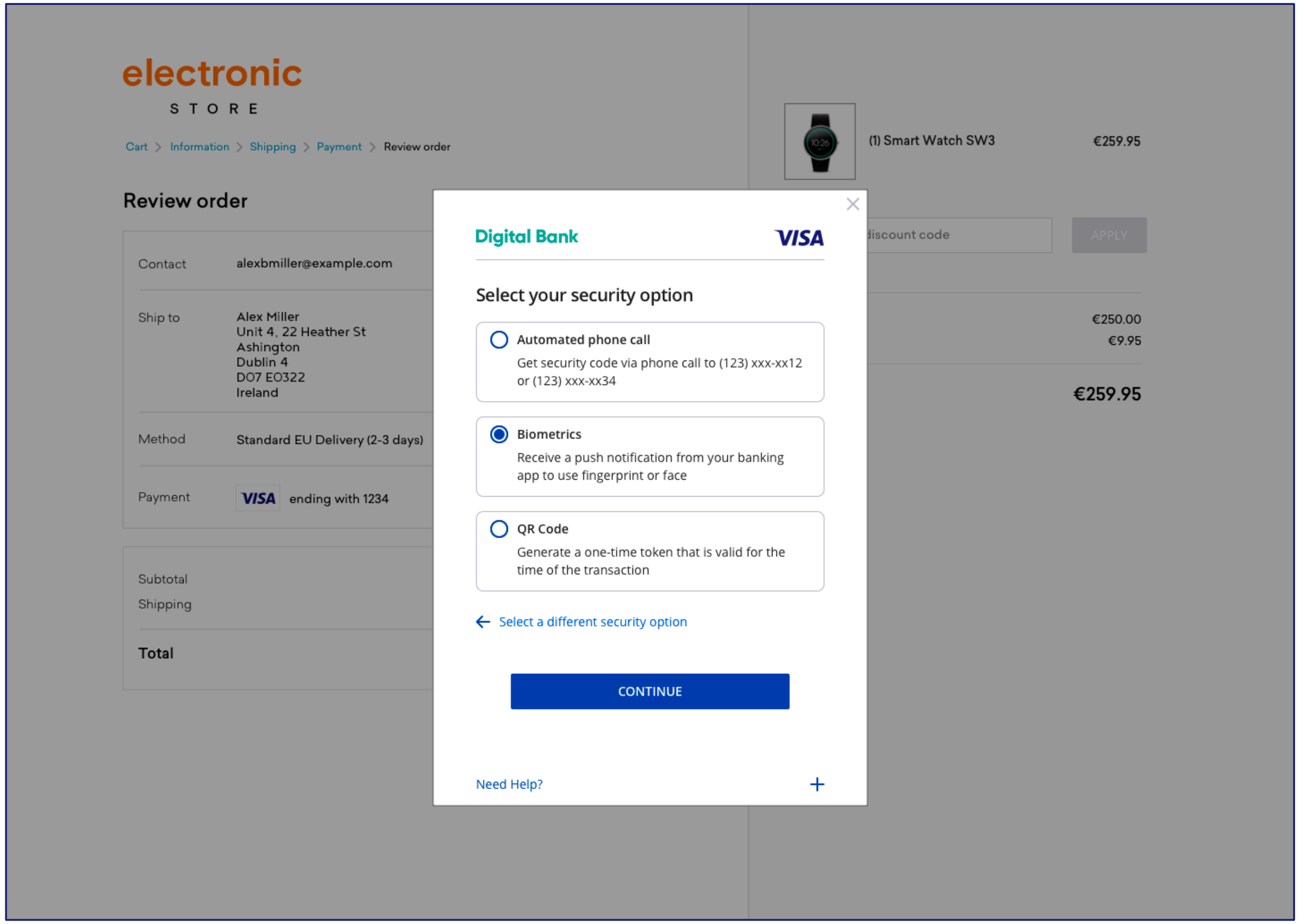
2.2 Customer experience online

Here's how your customers will make Visa payments once SCA is live:

Step 2.

To complete the transaction, they can choose their verification method or follow their Issuer's chosen method.

Tip:
If a customer contacts you about issues regarding authentication, refer them to their Issuer for more information.



electronic
STORE

Cart > Information > Shipping > Payment > Review order

Review order

Contact	alexbmiller@example.com
Ship to	Alex Miller Unit 4, 22 Heather St Ashington Dublin 4 D07 E0322 Ireland
Method	Standard EU Delivery (2-3 days)
Payment	VISA ending with 1234

Subtotal
Shipping

Total

(1) Smart Watch SW3 €259.95

discount code APPLY

€250.00
€9.95

€259.95

Digital Bank VISA

Select your security option

○ Automated phone call
Get security code via phone call to (123) xxx-xx12 or (123) xxx-xx34

● Biometrics
Receive a push notification from your banking app to use fingerprint or face

○ QR Code
Generate a one-time token that is valid for the time of the transaction

← Select a different security option

CONTINUE

Need Help? +

Electronic store is an example Merchant created to demonstrate the purchase process only.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

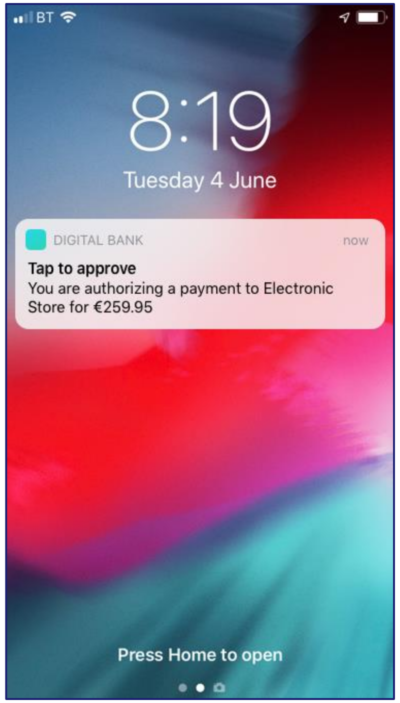
2.2 Customer experience online

Here’s how your customers will make Visa payments once SCA is live:

Step 3.

They simply need to follow the instructions to complete their purchase.

Tip:
If a customer contacts you about issues regarding authentication, refer them to their Issuer for more information.

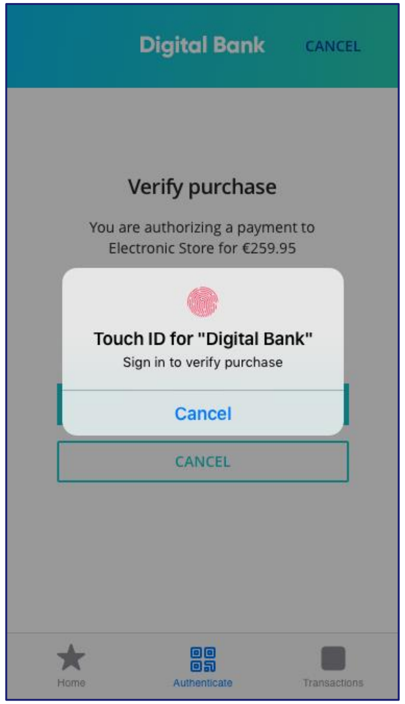


8:19

Tuesday 4 June

DIGITAL BANK now

Tap to approve
You are authorizing a payment to Electronic Store for €259.95



Digital Bank CANCEL

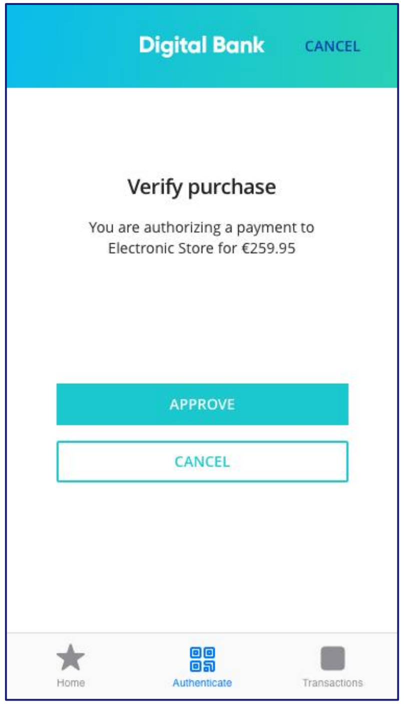
Verify purchase

You are authorizing a payment to Electronic Store for €259.95

Touch ID for "Digital Bank"
Sign in to verify purchase

Cancel

CANCEL



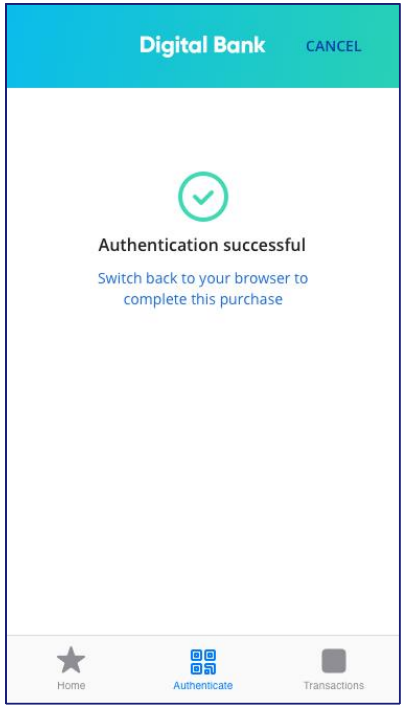
Digital Bank CANCEL

Verify purchase

You are authorizing a payment to Electronic Store for €259.95

APPROVE

CANCEL



Digital Bank CANCEL

Authentication successful

Switch back to your browser to complete this purchase

Electronic store is an example Merchant created to demonstrate the purchase process only.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

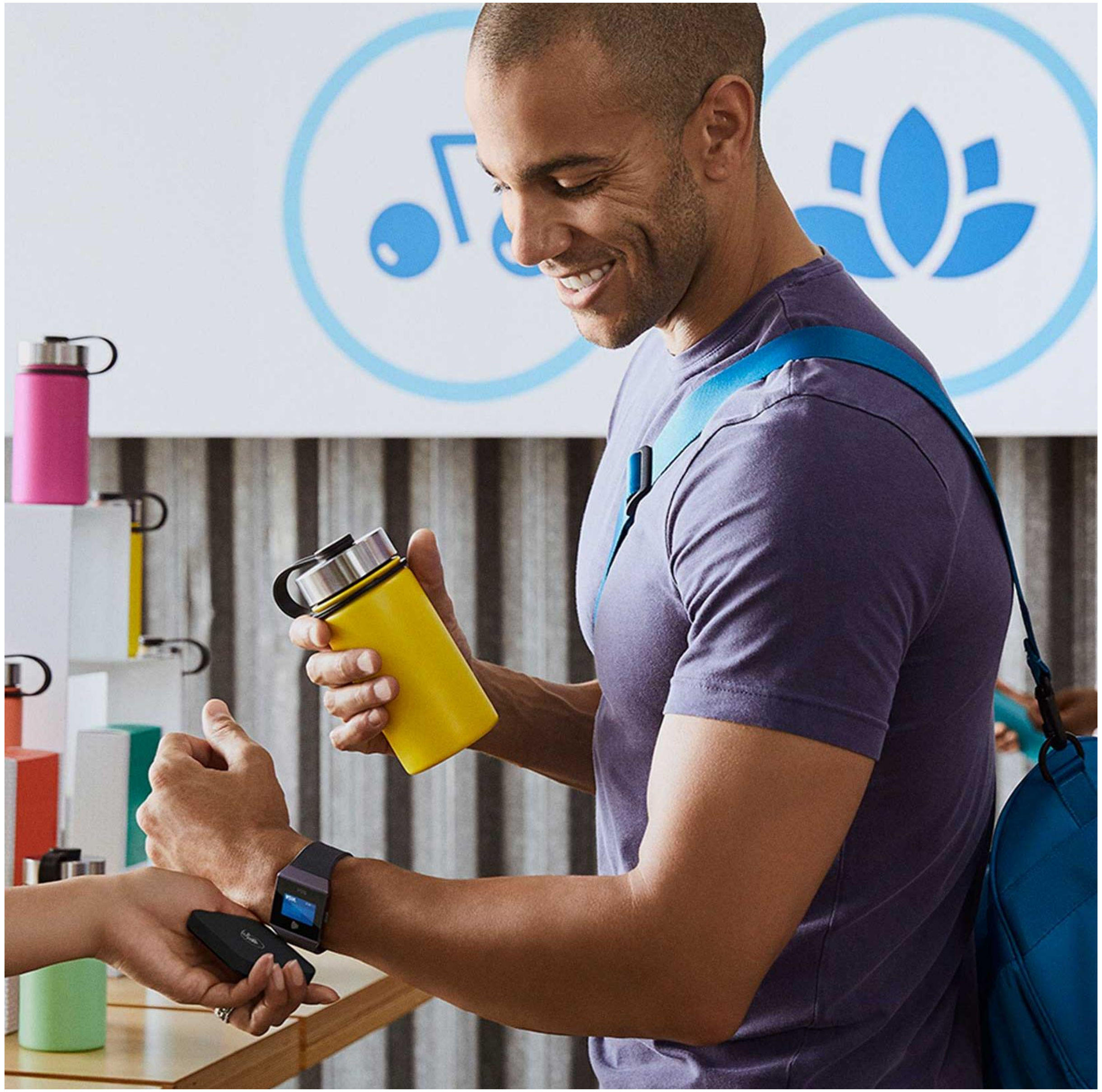
2.3 Customer experience in-store

Customers may have to enter their PIN more often when they pay contactless if:

- Customers are making more than (5)** consecutive contactless purchases without providing authentication or;
- The cumulative value of contactless payments since the last time additional authentication was provided exceeds (€150)** in total or;
- An Issuer wishes to verify the customer.

Tip:
If the customer is unable to complete the contactless transaction after entering their PIN, advise them to insert their card and enter their PIN to perform a chip and PIN payment.

If the problem persists, please tell them to speak to their Issuer, which will be able to provide more information.



**Dependent on Issuer implementation

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3. Implementing SCA

3.1 Speaking to your PSP

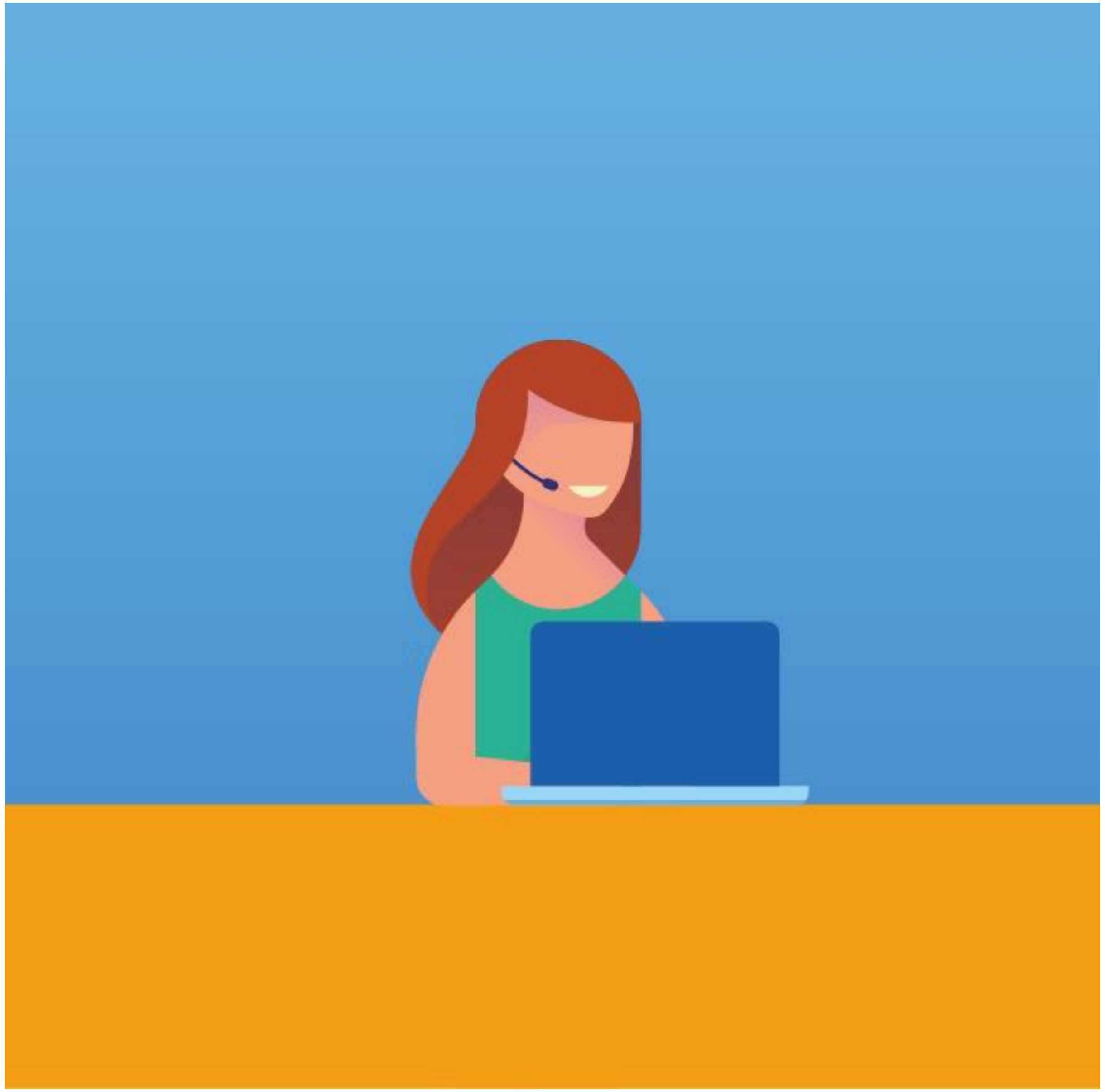
Merchants such as your business have a role to play in reducing fraud and improving customer experience.

Therefore, your business needs to be ready for SCA to avoid issuing banks declining transactions wherever possible.

Find out from your PSP:

- what you need to do
- what this will mean for your business
- how to support a frictionless payment experience for customers.

The next sections outline what you may need to discuss with them whether your business operates online, in-store or both and you want to benefit from the SCA exemptions.



This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3.2 Implementation for online businesses

You will need to speak to your PSP to help you navigate the changes from a technology perspective to process online payments.

Contact your PSP:
Once you have implemented 3DS through your PSP, your PSP will supply you with the 'Visa Secure' badge (signage) for your online shop.

To promote a great online payment experience for your customers:

- Ensure you have enrolled to authenticate using **3-D Secure (3DS)** – Visa offers this service via Visa Secure. Without Visa Secure your customers may be unable to complete online transactions.
- Upgrade to the newest version of 3DS – the most up to date version is 3DS 2.2 – for the best customer experience especially when purchasing in-app and on smartphones. It also brings important advantages to your business.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3.3 Implementation for bricks and mortar businesses

In-store chip and PIN payments won’t change. For contactless payments, customers may need to enter their PIN more often.

Response codes
Currently, when your PSP processes a transaction, they send your business a 2-digit response code from the issuing bank to notify you of the payment status. The status will tell you that the payment was approved, declined or what action needs to be taken. These response codes will change following the introduction of SCA.

How will the response codes change?
During the transaction process, two new response codes will be activated in the following instances:

- Customers are making more than (5)** consecutive contactless purchases without providing authentication or;
- The cumulative value of contactless payments since the last time additional authentication was provided exceeds (€150)** in total or;
- An Issuer wishes to verify the customer.

PSPs are in control of the new response codes. If Issuers in any EEA country use the new response codes, PSPs and Merchants will need to be ready ensuring that their terminals can support the new codes:

Code 70

Code 1A

1. **Response code 70** – this applies to online PIN transactions and asks the customer to enter their PIN.

2. **Response code 1A** – this applies to offline PIN transactions and communicates to the terminal to switch the interface to insert card in the terminal and enter a PIN.

Contact your PSP
They can help you navigate the changes from a technology perspective.

**Dependent on Issuer implementation

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3.4 Take advantage of exemptions

Contact your PSP
Understand how your business can take advantage of SCA exemptions and out of scope transactions to offer a seamless payment experience to your customers.

Here are some examples of when customers won’t need to use two-factor authentication to make payments.

- **For contactless payments under** (€XX)* (However, after five consecutive transactions, or if cumulative value of contactless payments since the last time additional authentication was provided exceeds (€150)*, they may have to enter their PIN.)
- **Low-risk online payments.** As part of the new security measures, banks will be able to make better and faster risk analysis decisions as they will be provided with more extensive data. SCA is not required if an online payment is determined to be low risk using real-time transaction analysis.
- **Trusted merchants.** Cardholders can add a shop they trust to a list, so that they do not need to provide SCA when purchasing from that shop.**
- **Corporate payments.** Some corporate payments made through dedicated processes may be exempt, if the local regulator agrees they are sufficiently secure (e.g. lodge or virtual cards).

*Dependent on local market contactless limit. (CVM – customer Verification Method).
**Coming soon to your market. Check with your PSP.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3.4 Take advantage of exemptions

Contact your PSP
Understand how your business can take advantage of SCA exemptions and out of scope transactions to offer a seamless payment experience to your customers.

Here are some examples of when customers won’t need to use two-factor authentication to make payments.

- **Low value payments online.** Just like contactless, payments below (€XX) are exempt from SCA. (However, if the exemption has been used five times since the customer’s last successful authentication, or if payments exceed (€XX), their bank may request authentication.)

- **Unattended transport and parking terminals.** Any payment for transport fares or parking at unattended terminals (e.g. at an airport or train station) will not require SCA**.

**If an Issuer implements a ‘Card-Based Solution’ then SCA may be triggered in some unique cases, for which the cardholder will not be able to complete SCA requirements such as entering their PIN.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

3.5 Transactions where SCA does not apply (out of scope)

There are transactions where SCA does not apply. The list to the right is not exhaustive. Please refer to page 2.

- **Merchant Initiated Transactions (MIT).** These include subscriptions and instalments agreed in advance with the cardholder and initiated by the Merchant. When setting up a new subscription or membership, customers may be asked to authenticate.
- **Mail order/telephone payments.** Any payments made over the phone or via mail order will not require authentication.
- **A transaction where either the bank or PSP is located outside the EEA.** Your bank will still have to use its best efforts to apply SCA where possible.
- **Anonymous transactions.** SCA may not be needed if customers make a purchase with an anonymous prepaid card, which doesn’t require you to know the cardholder.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4. How to communicate to customers

4.1 How to explain SCA to your customers

For SCA to be a success, it’s vitally important that your staff and customers are aware of the improvements that are coming.

To help you communicate the improvements to your staff, we’ve created:

A conversation aid

Website messaging

A staff manual with FAQs

These should help your staff feel reassured and confident about the upcoming SCA developments.

The customer’s issuing bank will be best placed to provide detailed information on SCA such as anti-fraud measures and payment security. If your customer has specific queries about SCA, ensure your staff are prepared to refer the customer to their Issuer.

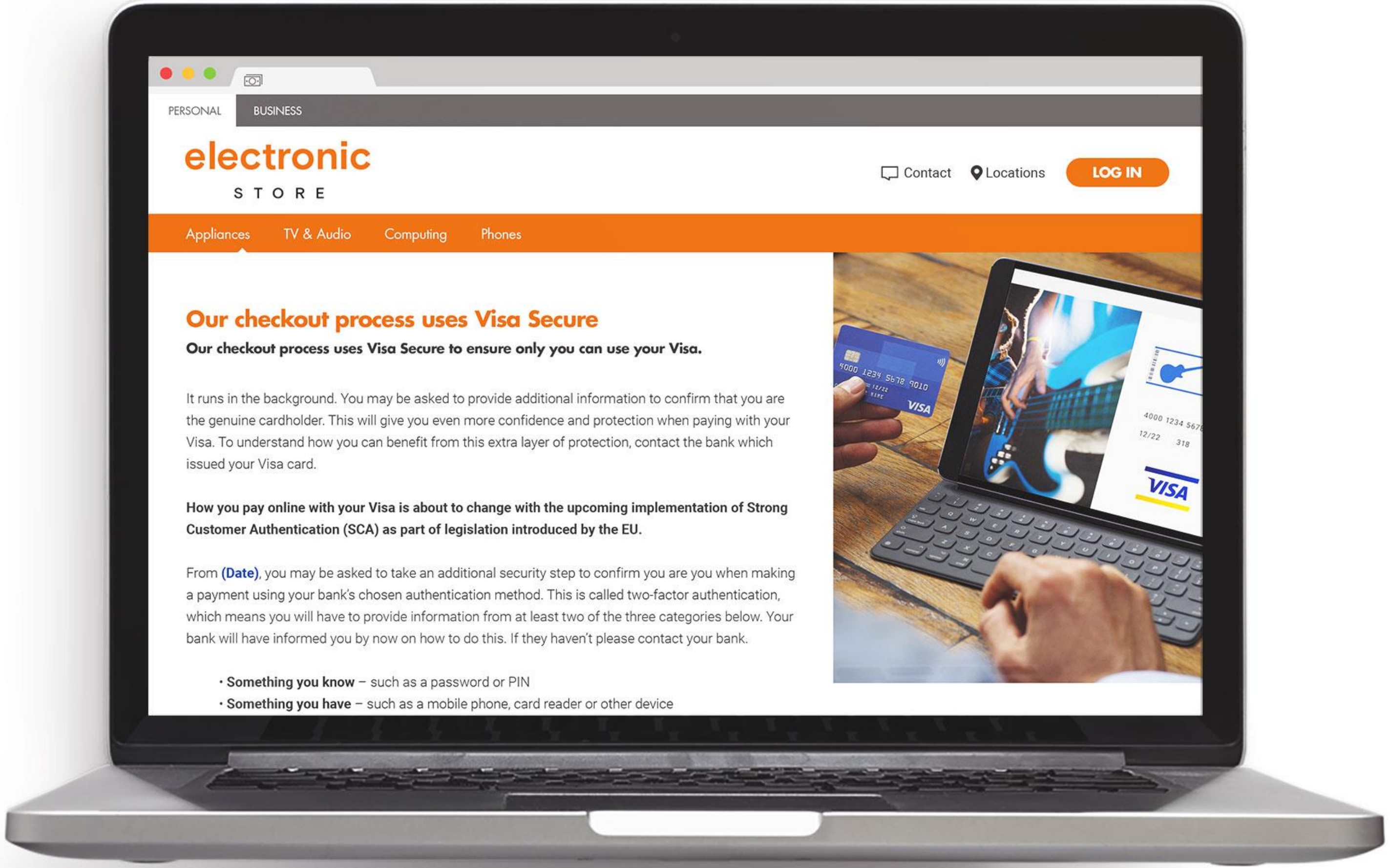
This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4.2 Marketing Communications Guidance for online businesses

4.2.1 Website paragraph

Here’s an example of how we would recommend you communicate SCA on your website, where you feel it’s appropriate (e.g. FAQ page, help page or during the checkout process).

Full copy here ›



Our checkout process uses Visa Secure

Our checkout process uses Visa Secure to ensure only you can use your Visa.

It runs in the background. You may be asked to provide additional information to confirm that you are the genuine cardholder. This will give you even more confidence and protection when paying with your Visa. To understand how you can benefit from this extra layer of protection, contact the bank which issued your Visa card.

How you pay online with your Visa is about to change with the upcoming implementation of Strong Customer Authentication (SCA) as part of legislation introduced by the EU.

From **(Date)**, you may be asked to take an additional security step to confirm you are you when making a payment using your bank’s chosen authentication method. This is called two-factor authentication, which means you will have to provide information from at least two of the three categories below. Your bank will have informed you by now on how to do this. If they haven’t please contact your bank.

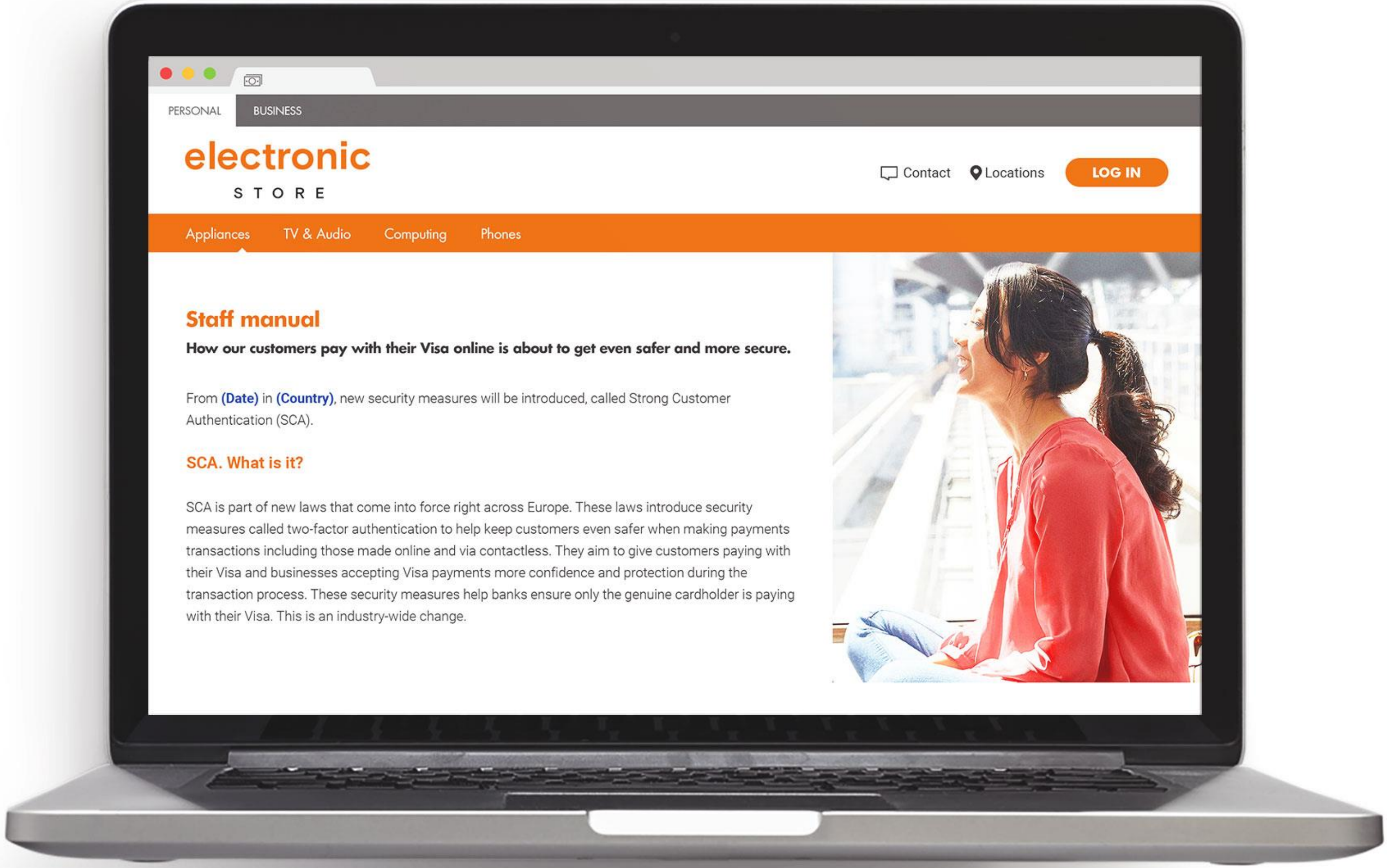
- **Something you know** – such as a password or PIN
- **Something you have** – such as a mobile phone, card reader or other device

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4.2.2 Staff manual

Here’s an example of a staff manual which shows how we would recommend you communicate SCA to your staff. It gives the background information needed to help answer some common customer questions and will help avoid any disruption to your business.

Full copy here ›



Staff manual

How our customers pay with their Visa online is about to get even safer and more secure.

From **(Date)** in **(Country)**, new security measures will be introduced, called Strong Customer Authentication (SCA).

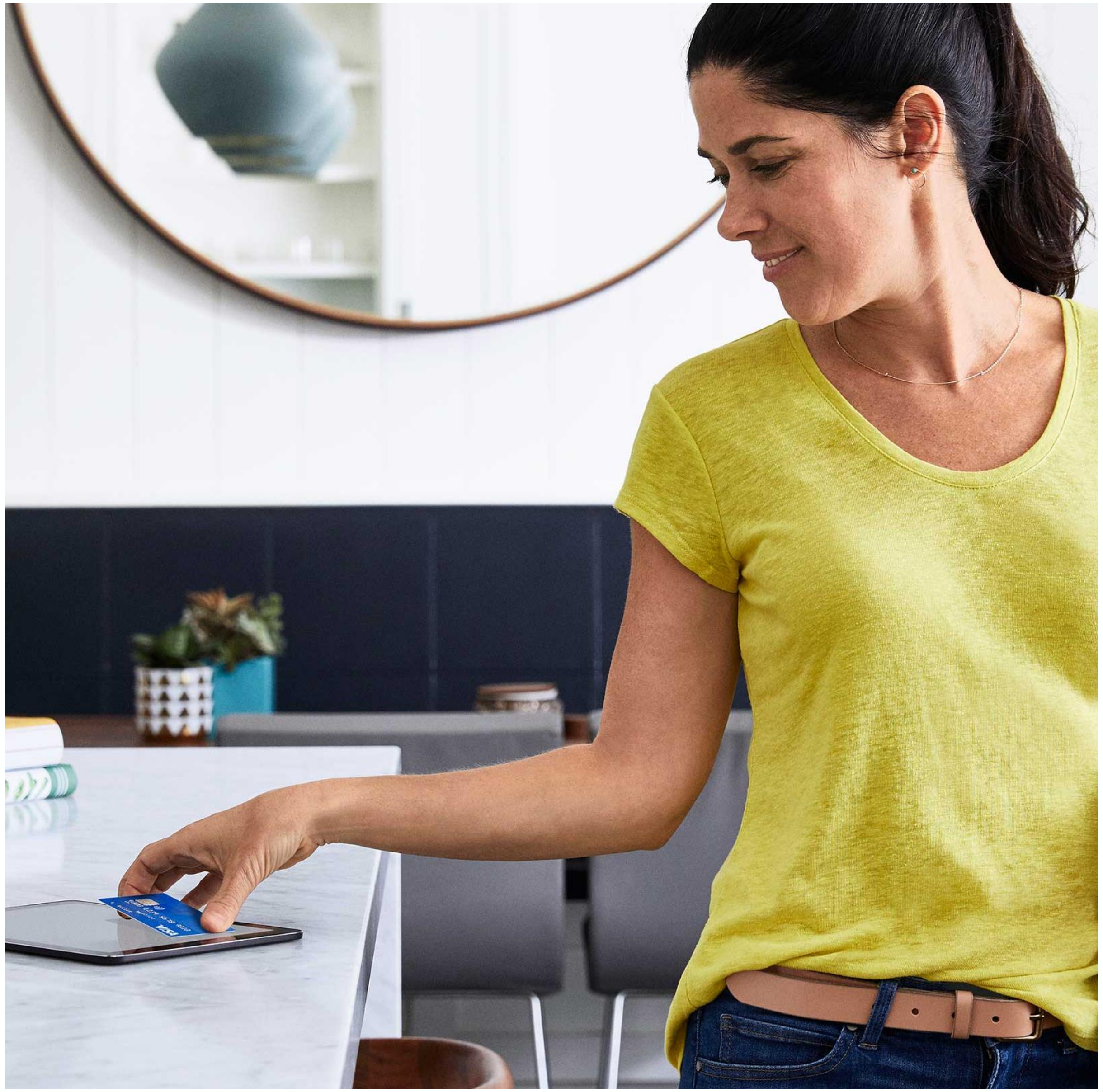
SCA. What is it?

SCA is part of new laws that come into force right across Europe. These laws introduce security measures called two-factor authentication to help keep customers even safer when making payments transactions including those made online and via contactless. They aim to give customers paying with their Visa and businesses accepting Visa payments more confidence and protection during the transaction process. These security measures help banks ensure only the genuine cardholder is paying with their Visa. This is an industry-wide change.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4.2.3 Website call-out

You can use the Visa Secure badge on your website. When your customers see ‘Visa Secure’, they can be sure their transaction is protected by multiple layers of security. Contact your PSP to obtain the badge.



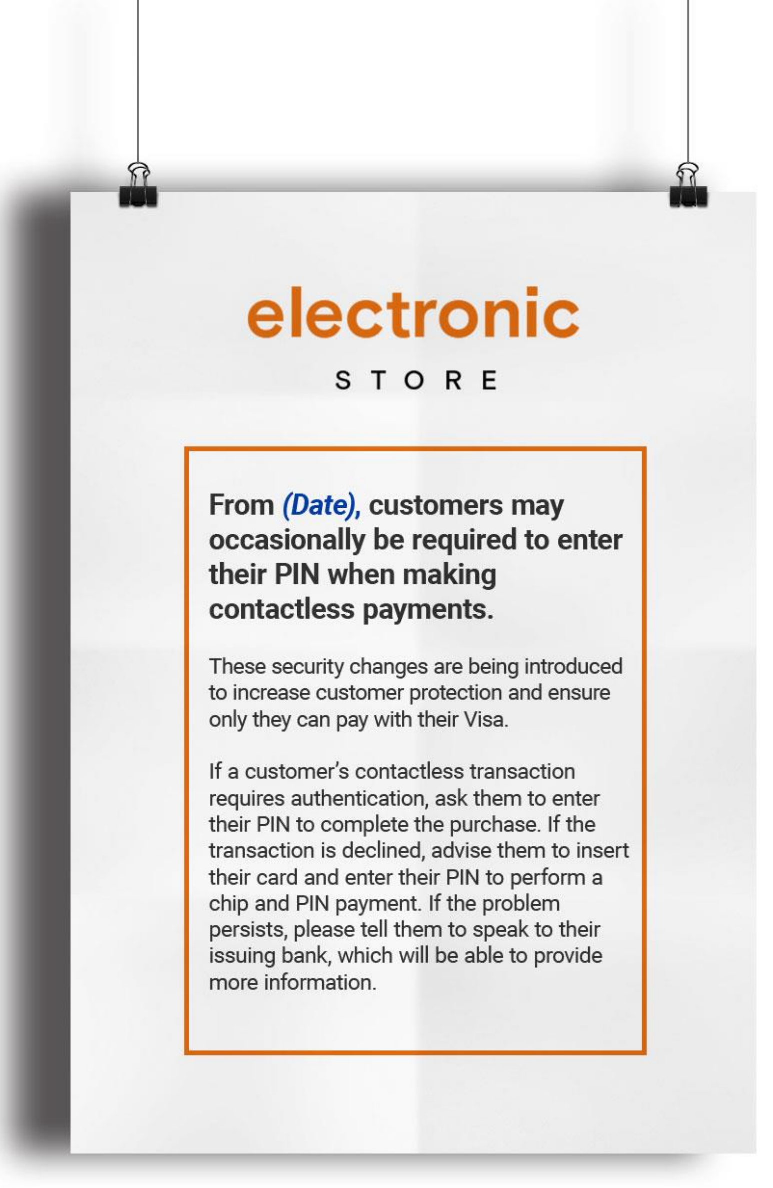
This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4.3 Marketing Communications Guidance for bricks and mortar businesses

4.3.1 Conversation aid

Here’s an example of a more concise version of the staff manual. It highlights how we would recommend you communicate SCA to your staff. This can go by the till(s) in-store and assist any new employees who haven’t been trained yet.

Full copy here ›



electronic

STORE

From *(Date)*, customers may occasionally be required to enter their PIN when making contactless payments.

These security changes are being introduced to increase customer protection and ensure only they can pay with their Visa.

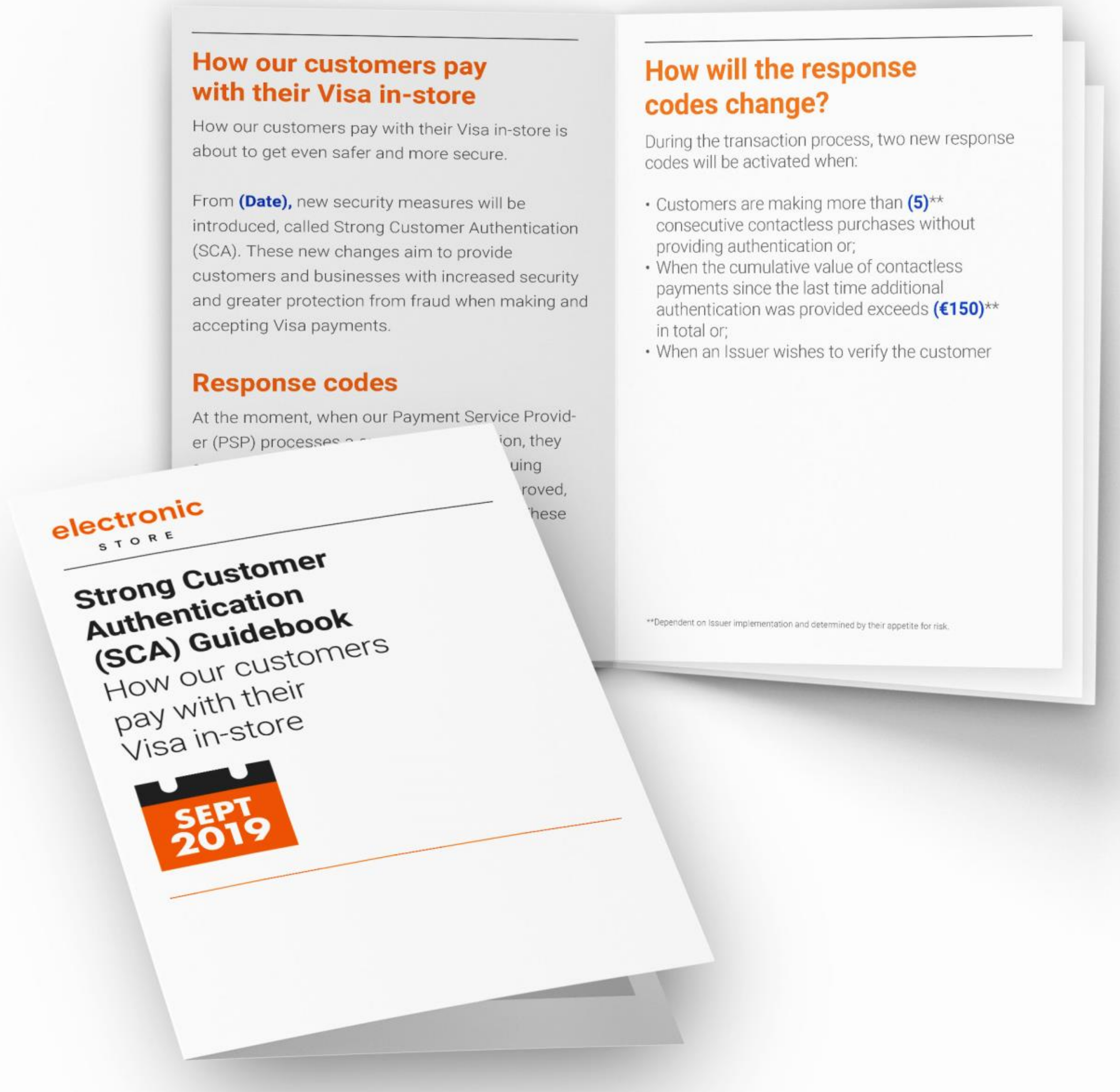
If a customer’s contactless transaction requires authentication, ask them to enter their PIN to complete the purchase. If the transaction is declined, advise them to insert their card and enter their PIN to perform a chip and PIN payment. If the problem persists, please tell them to speak to their issuing bank, which will be able to provide more information.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

4.3.2 Staff manual

Here’s an example of how we would recommend you communicate SCA to your staff. It gives them the background information and shows them how to answer some common customer questions.

Full copy here >



How our customers pay with their Visa in-store

How our customers pay with their Visa in-store is about to get even safer and more secure.

From **(Date),** new security measures will be introduced, called Strong Customer Authentication (SCA). These new changes aim to provide customers and businesses with increased security and greater protection from fraud when making and accepting Visa payments.

Response codes

At the moment, when our Payment Service Provider (PSP) processes a … ion, they … uing … roved, … hese

How will the response codes change?

During the transaction process, two new response codes will be activated when:

- Customers are making more than **(5)**** consecutive contactless purchases without providing authentication or;
- When the cumulative value of contactless payments since the last time additional authentication was provided exceeds **(€150)**** in total or;
- When an Issuer wishes to verify the customer

**Dependent on Issuer implementation and determined by their appetite for risk.

electronic
STORE

Strong Customer Authentication (SCA) Guidebook

How our customers pay with their Visa in-store

SEPT 2019

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix: Detailed Communications Material

Here you'll find some recommended communications for cardholders.

These are guiding documents that you can use in your messaging.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.2.1

‹ BACK

Website paragraph

Here's an example of how we would recommend you communicate SCA on your business website, where you feel it's appropriate (e.g. FAQ page, help page or during the checkout process).

Our checkout process uses Visa Secure
Our checkout process uses Visa Secure to ensure only you can use your Visa. It runs in the background. You may be asked to provide additional information to confirm that you are the genuine cardholder. This will give you even more confidence and protection when paying with your Visa. To understand how you can benefit from this extra layer of protection, contact the bank which issued your Visa card.

How you pay online with your Visa is about to change with the upcoming implementation of Strong Customer Authentication (SCA) as part of legislation introduced by the EU.

From **(Date)***, you may be asked to take an additional security step to confirm you are you when making a payment using your bank's chosen authentication method. This is called two-factor authentication, which means you will have to provide information from at least two of the three categories below. Your bank will have informed you by now on how to do this. If they haven't please contact your bank.

- **Something you know** – such as a password or PIN
- **Something you have** – such as a mobile phone, card reader or other device
- **Something you are** – such as iris scans, facial recognition or a fingerprint

Include this section if your business offers subscriptions or recurring payments.
You may need to confirm you are you when setting up a new subscription or recurring payment. Subsequent payments and existing subscriptions will not require two-factor authentication, although authentication may be needed if you make changes to your subscription.

*Insert date as required

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.2.2 ‹BACK

Staff manual

Here’s an example of a staff manual which shows how we would recommend you communicate SCA to your staff. It gives them the background information needed to help answer some common customer questions and will help avoid any disruption to your business.

How our customers pay with their Visa online is about to get even safer and more secure.

New security measures will be introduced, called Strong Customer Authentication (SCA).

SCA. What is it?
SCA is part of new laws that come into force right across Europe. These laws introduce security measures called two-factor authentication to help keep customers even safer when making payments transactions including those made online and via contactless. They aim to give customers paying with their Visa and businesses accepting Visa payments more confidence and protection during the transaction process. These security measures help banks ensure only the genuine cardholder is paying with their Visa. This is an industry-wide change.

How will it work when you shop with us?
When a customer pays with their Visa, they may be asked to take an additional security step to confirm who they are using their bank’s chosen authentication method. This is called two-factor authentication, which means they will have to provide information from at least two of the three categories below:

- **Something they know** – such as a password or PIN
- **Something they have** – such as a mobile phone, card reader or other device
- **Something they are** – such as iris scans, facial recognition or a fingerprint

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.2.2 ‹BACK

Staff manual

Here's an example of a staff manual which shows how we would recommend you communicate SCA to your staff. It gives them the background information needed to help answer some common customer questions and will help avoid any disruption to your business.

Include if your business offers subscriptions or recurring payments.

How will customers set up a new subscription or recurring payment?

When setting up a new subscription, customers may be asked to confirm who they are through their bank's chosen two-factor authentication method. Subsequent payments and existing subscriptions will not require two-factor authentication, although authentication may be needed if you make changes to your subscription.

What will SCA mean for our customers?

From this date, the way our customers pay online may change because of two-factor authentication.
The increased levels of security will benefit them by increasing their trust and confidence while shopping online. They will also be able to pay using a range of devices such as smartphones, tablets, and laptops, for an improved customer experience.

As part of the changes, banks will receive more data to make better informed decisions and assess whether a transaction is low risk (exempted) or out of scope of SCA. This will help to create a more frictionless payment experience by reducing fraud risk and the number of times cardholders need to authenticate their Visa payment.

What do we need to do?

We all need to be informed about the changes that SCA will bring, so we can raise awareness and assist our customers. However, if they have any queries that you're unable to answer, please direct them to their issuing bank, which will be able to provide more information.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.2.2

‹BACK

Staff manual

Here's an example of a staff manual which shows how we would recommend you communicate SCA to your staff. It gives them the background information needed to help answer some common customer questions and will help avoid any disruption to your business.

FAQs

1. **What is SCA?**
   SCA stands for 'Strong Customer Authentication'. From **(Date),** banks will be bringing in new security measures as part of new laws that come into force across Europe for card payments. They will make paying with Visa even safer because of two-factor authentication, which offers an added layer of security when making online and contactless payments. It will help banks ensure only the genuine cardholder can use their Visa.

2. **How will our customers pay online when SCA goes live?**
   They may be asked to take an additional security step to confirm who they are using their bank's chosen authentication method. They will have to provide information from at least two of the three categories below:

- **Something they know** – such as a password or PIN
- **Something they have** – such as a mobile phone, card reader or other device
- **Something they are** – such as iris scans, facial recognition or a fingerprint

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.2.2

‹ BACK

Staff manual

Here's an example of a staff manual which shows how we would recommend you communicate SCA to your staff. It gives them the background information needed to help answer some common customer questions and will help avoid any disruption to your business.

Include this FAQ if your business offers subscriptions or recurring payments.

3. **What will happen when our customers set up a new subscription or recurring payment?**
   Our customers may be asked to verify themselves once when setting up a new subscription or new recurring payment through their bank's chosen method. Subsequent payments and existing subscriptions will not require two-factor authentication, although authentication may be needed if you make changes to your subscription

4. **What should our customers do if their transaction is declined or they don't know how to authenticate?**
   Tell them to speak to their bank. They will be able to offer your customer more information.

5. **What is Visa Secure?**
   Visa Secure is the technology banks use to make our customers' payments more secure. When our customers see 'Visa Secure' online, they can be sure their transaction is protected by multiple layers of security. And they'll be protected by Visa's zero liability policy if anyone makes a fraudulent transaction with their Visa.

6. **Is this extra security free?**
   Yes. There's no charge levied by Visa on Merchants for this new layer of protection.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.3.1 ‹BACK

Conversation aid

Here's an example of a more concise version of the staff manual and highlights how we would recommend you communicate SCA to your staff. This can go by the till(s) in-store and assist any new employees who haven't been trained yet.

From **(Date)***, customers may occasionally be required to enter their PIN when making contactless payments.

These security changes are being introduced to increase customer protection and ensure only they can pay with their Visa.

If a customer's contactless transaction requires authentication, ask them to enter their PIN to complete the purchase. If the transaction is declined, advise them to insert their card and enter their PIN to perform a chip and PIN payment. If the problem persists, please tell them to speak to their issuing bank, which will be able to provide more information.

*Insert date as required

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Appendix 4.3.2 ‹BACK

Staff manual

Here’s an example of how we would recommend you communicate SCA to your staff. It gives them the background information and shows them how to answer some common customer questions.

How our customers pay with their Visa in-store
How our customers pay with their Visa in-store is about to get even safer and more secure.

From **(Date)***, new security measures will be introduced, called Strong Customer Authentication (SCA). These new changes aim to provide customers and businesses with increased security and greater protection from fraud when making and accepting Visa payments.

Response codes
At the moment, when our Payment Service Provider (PSP) processes a customer transaction, they send a 2-digit response code from the issuing bank to tell us if the payment has been approved, declined or what action needs to be taken. These response codes will change following SCA.

How will the response codes change?
During the transaction process, two new response codes will be activated when:

- Customers are making more than (5)** consecutive contactless purchases without providing authentication or;
- When the cumulative value of contactless payments since the last time additional authentication was provided exceeds (€150)** in total or;
- When an Issuer wishes to verify the customer

*Insert date as required
**Dependent on Issuer implementation

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Staff manual

Here's an example of how we would recommend you communicate SCA to your staff. It gives them the background information and shows them how to answer some common customer questions.

Include in FAQs if the below is relevant for your staff

Banks are in control of the new response codes. For our business to be ready by **(Date)***, we will need to ensure that all our terminals can support these two new codes:

1. **Response code 70** – this applies to online PIN transactions and asks the customer to enter their PIN.
2. **Response code 1A** – this applies to offline PIN transactions and communicates to the terminal to switch the interface to insert card in the terminal and enter a PIN.

FAQs

1. What is SCA?

SCA stands for 'Strong Customer Authentication'. Banks will be bringing in new security measures as part of new laws that come into force across Europe. They will make paying with Visa even safer because of two-factor authentication, which offers an added layer of security when paying with contactless. It will help banks ensure only the cardholder can use their Visa.

2. What will happen when customers shop in-store with contactless?

In-store, they may be asked to enter their PIN more often.

3. What should customers do if their contactless transaction is declined?

Advise the customer to insert their card and enter their PIN to perform a chip and PIN payment. If the transaction fails or returns declined, please tell the customer to speak to their issuing bank. They will be able to offer more information.

*Insert date as required

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Staff manual

Here’s an example of how we would recommend you communicate SCA to your staff. It gives them the background information and shows them how to answer some common customer questions.

4. **What is Visa Secure?**
   Visa Secure is the technology banks use to make the customer’s payment more secure. When they see ‘Visa Secure’ online, they can be sure their transaction is protected by multiple layers of security.

5. **How does Visa protect customers?**
   They’ll be protected by Visa’s zero liability policy if anyone makes a fraudulent transaction with their Visa.

6. **Is this extra security free?**
   Yes. There’s no charge levied by Visa on Merchants for this new layer of protection.

If you are a Merchant, which operates an online and offline business, please combine these materials as needed.

This material is not legal or other professional advice. Payment Service Providers are responsible for their own compliance with PSD2 requirements and their own customer communications. This material must be read together with slide 2.
This guidebook was published in September 2019.

Thank you

VISA everywhere you want to be