VISA

Strong Customer Authentication:

Marketing Communications guidebook for Merchants in CEMEA SCA countries

June 2024

Disclaimers

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.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Visa is not liable for any informational errors, incompleteness, or delays, or for any actions taken in reliance on information contained herein. 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.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Hello

We've created this guidebook to help your business prepare for the rollout of Strong Customer Authentication (SCA) in your country.

SCA aims to benefit everyone who makes and accepts Visa payments. It should result in 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 Acquiring partner.

In this Guidebook under the "Acquiring partner" we mean either your Bank-Acquirer or other Payment Service Provider (PSP) where applicable.

It also contains materials to help you raise awareness of the changes on your website and in-store to customers.

VISA

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Content

1. Understanding SCA

1.1 SCA in a nutshell

1.2 Two-factor authentication

1.3 Potential impact of SCA for your business

1.4 What you need to consider about SCA

2. SCA Customer experience

2.1 What SCA means for your customers

2.2 Customer experience online

2.3 Customer experience in-store

3. Implementing SCA

3.1 Speaking to your Acquiring partner

3.2 Implementation for online businesses

3.3 Implementation for in-store businesses

3.4 Take advantages for exemptions

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

3.6 Account verification transactions

4. How to communicate to customers

4.1 How to explain SCA to your customers

4.2 Marketing communications guidance for online businesses

4.3 Marketing communications for in-store businesses

Appendix:

Detailed Communications Material

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Understanding SCA

1.1 SCA in a nutshell

Strong customer authentication (SCA) requirements for electronic payments are being implemented into local laws of certain CEMEA countries.

The CEMEA SCA countries subject to these requirements currently are: Albania, Azerbaijan, Georgia, Moldova, Montenegro, North Macedonia and Ukraine. This list may be extended in accordance with local laws requirements.

These countries are referred to as "CEMEA countries subject to SCA requirements," or "CEMEA SCA countries" for short.

It will affect all businesses based or serving customers in the CEMEA SCA countries which accept card payments.

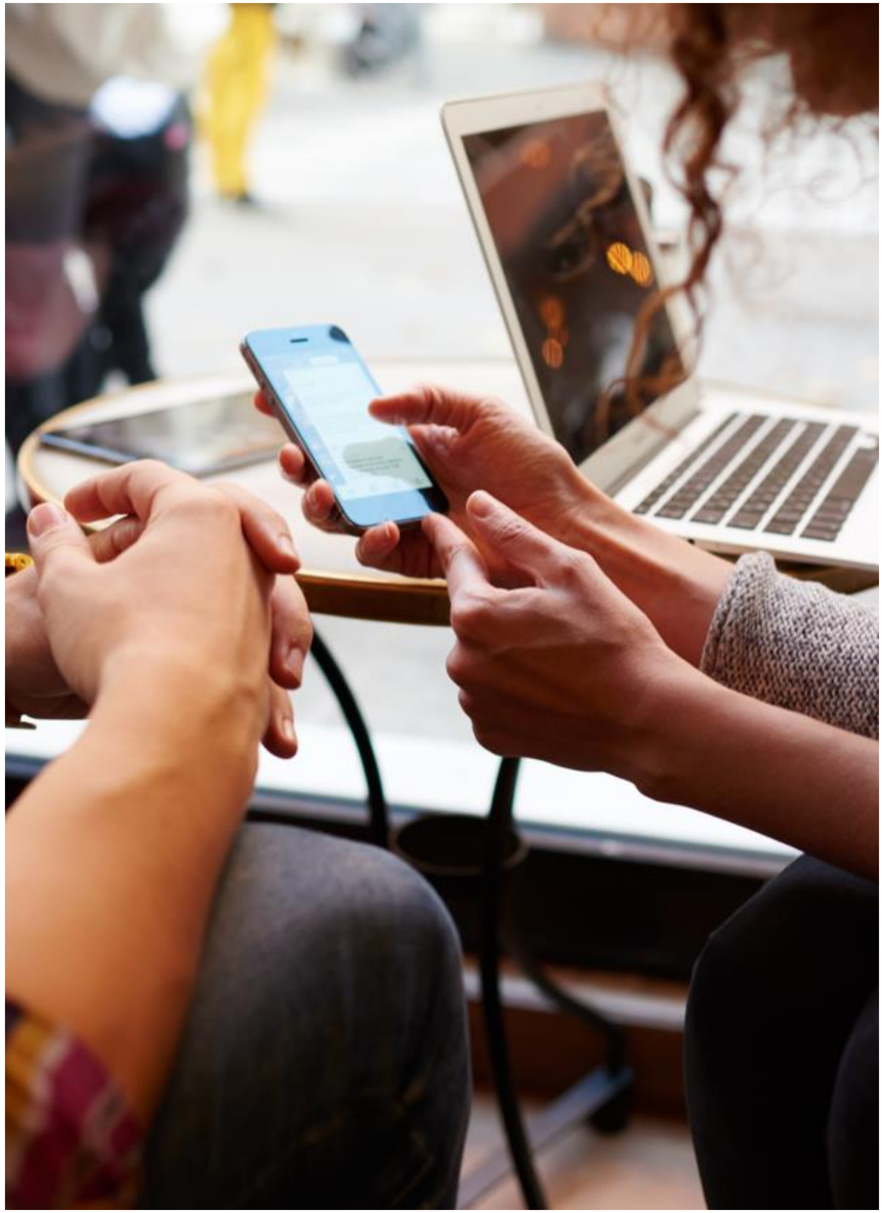
These laws introduce security measures called two-factor authentication to help keep customers even safer when making payments transactions including those made online and via contactless. This is an industry-wide change.

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 to create a more secure payment experience

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

Visa is working closely with participating Issuers and Acquirers to help protect customers.



This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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 card. This is called **two-factor authentication,** which means they may have to provide information from at least two out of the three categories below. What they will have to provide will depend on their bank's requirements.

Possession

Something only the payer has e.g.:

- Pre-registered mobile phone
- Card
- Key generation device
- OTP generated by, or received on, a device

Inherence

Something the payer is e.g.:

- A selfie
- A fingerprint
- Voice recognition

Knowledge

Something only the payer knows e.g.:

- A password
- A PIN
- Questions whose answers are only known to the payer

Your Acquiring partner can tell you what you need to do to get ready, and about the implementation timelines. Your Acquiring partner may also have information on the changes on their website.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

1.3 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 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 – Issuers expect to request customer authentication on more transactions.

Be prepared for SCA–businesses need to be prepared for SCA.

Keep your customer experience seamless to keep them coming back – contact your Acquiring partner to discuss the improvements that need to be made to build the new authentication process into customer`s Visa payment journey.

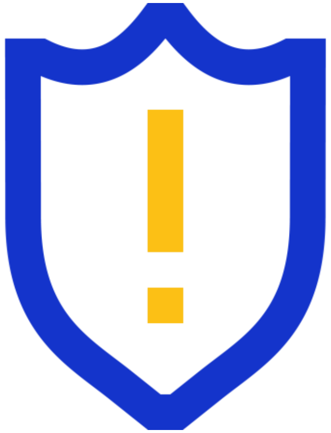
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

1.4 What you need to consider about SCA

You and your Acquiring partner 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 optimize your customers' payment experience and make the most of the opportunities SCA offers.

Visa's endeavors 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.



This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

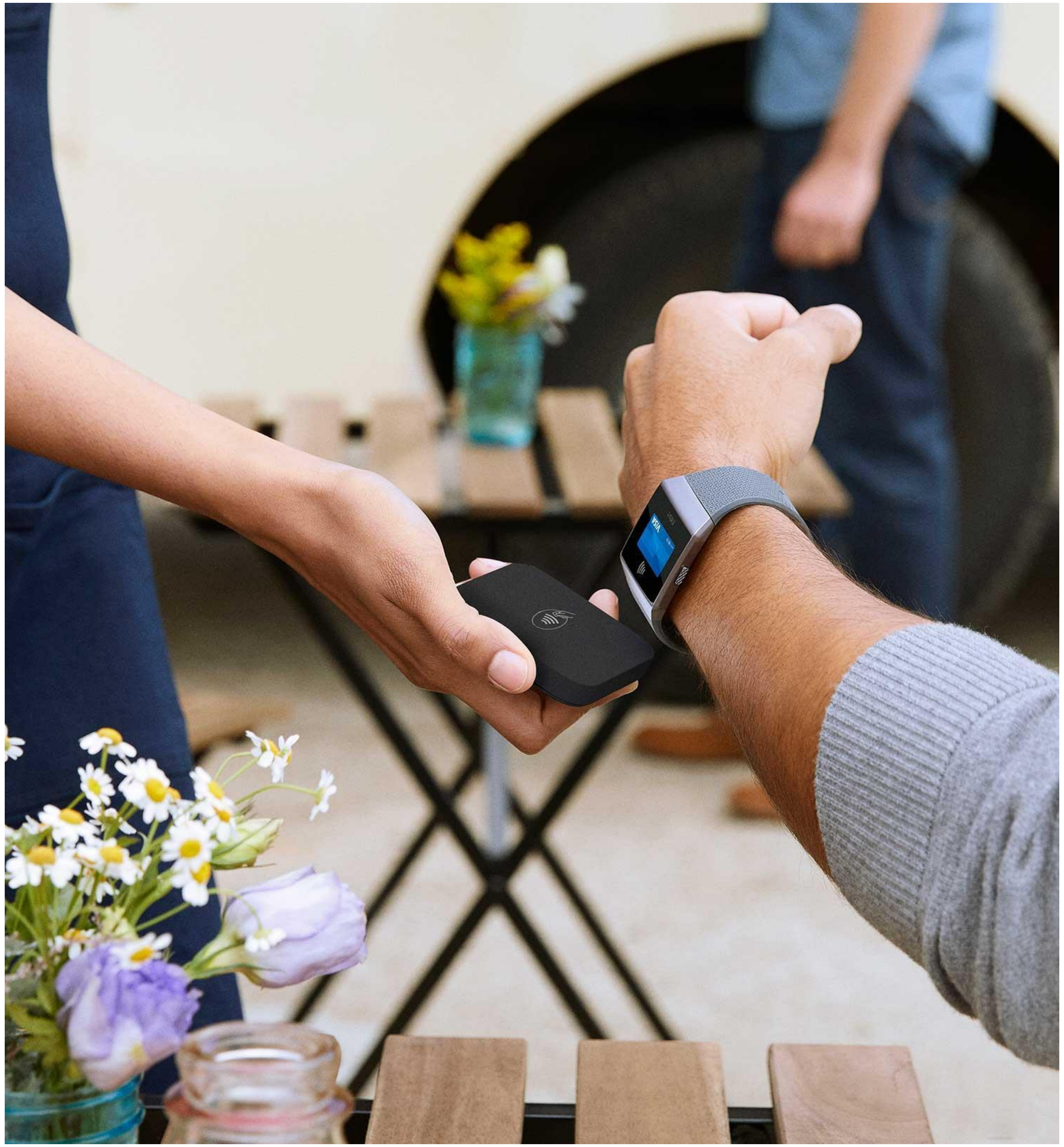
SCA Customer experience

experience

2.1 What SCA means 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 secure checkouts.



VISA

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

2.2 Customer experience online

Online
Here`s how your customers will make Visa payments when SCA is required

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

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

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

Something they know – such as a password or PIN

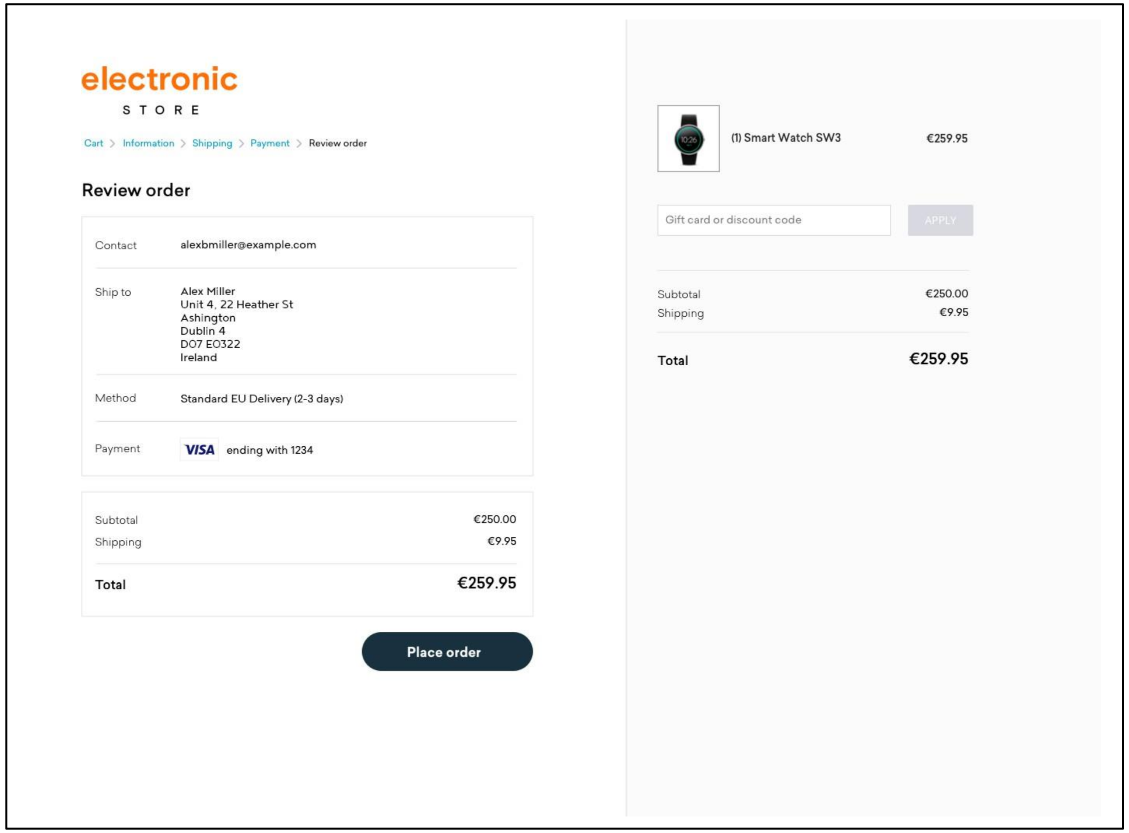
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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.


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

Gift card or discount code
APPLY

Subtotal	€250.00
Shipping	€9.95
Total	€259.95

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

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

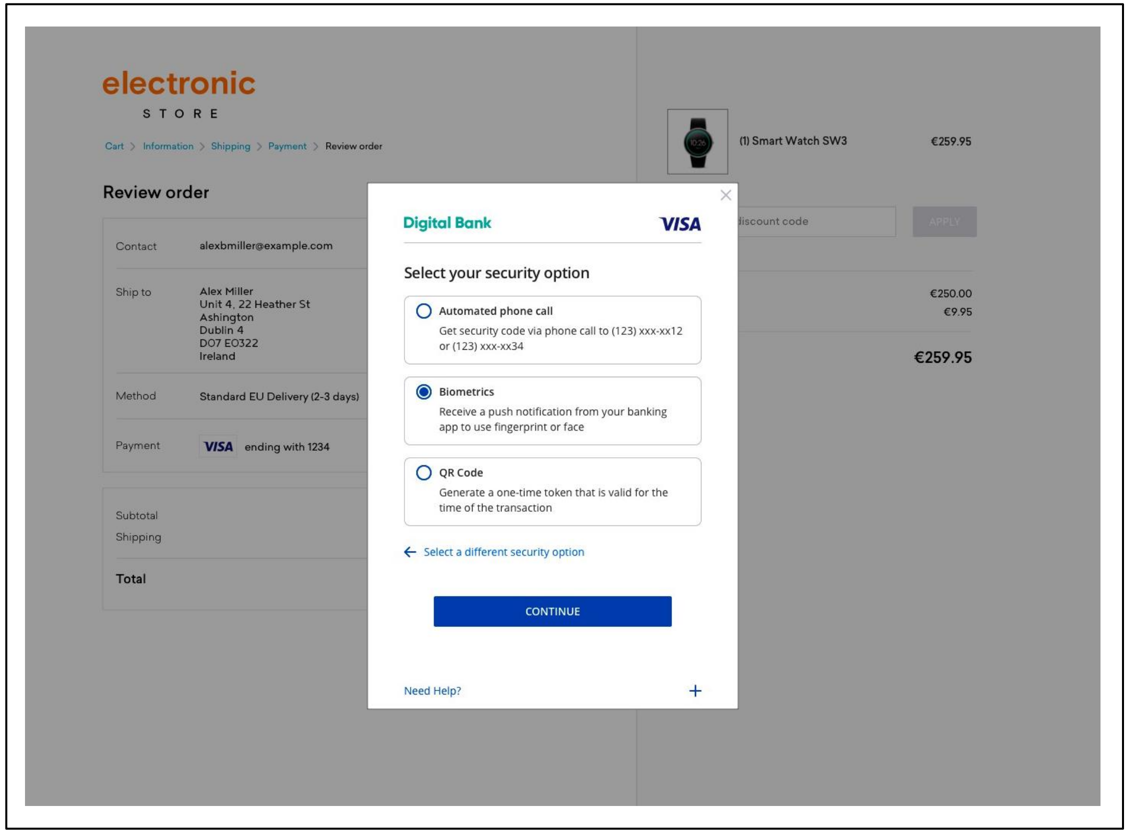
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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.


electronic
STORE
Cart > Information > Shipping > Payment > Review order
Digital Bank
VISA
discount code
APPLY
Select a different security option
CONTINUE
Need Help?
+

Review order

Contact	alexbmiller@example.com
Ship to	Alex Miller Unit 4, 22 Heather St Ashington Dublin 4 DO7 EO322 Ireland
Method	Standard EU Delivery (2-3 days)
Payment	VISA ending with 1234

(1) Smart Watch SW3		€259.95
Subtotal		€250.00
Shipping		€9.95
Total		€259.95

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

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

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

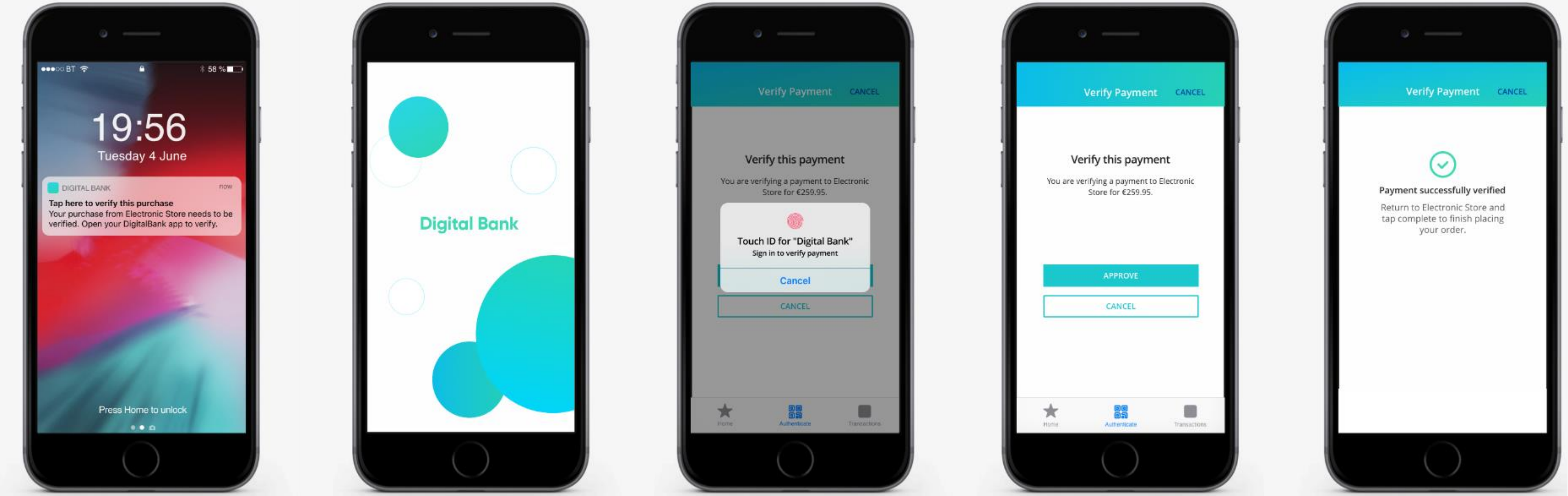
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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.



●●●○○ BT 58 %

19:56

Tuesday 4 June

DIGITAL BANK now

Tap here to verify this purchase

Your purchase from Electronic Store needs to be verified. Open your DigitalBank app to verify.

Press Home to unlock

Digital Bank

Verify Payment CANCEL

Verify this payment

You are verifying a payment to Electronic Store for €259.95.

Touch ID for "Digital Bank"

Sign in to verify payment

Payment successfully verified

Return to Electronic Store and tap complete to finish placing your order.

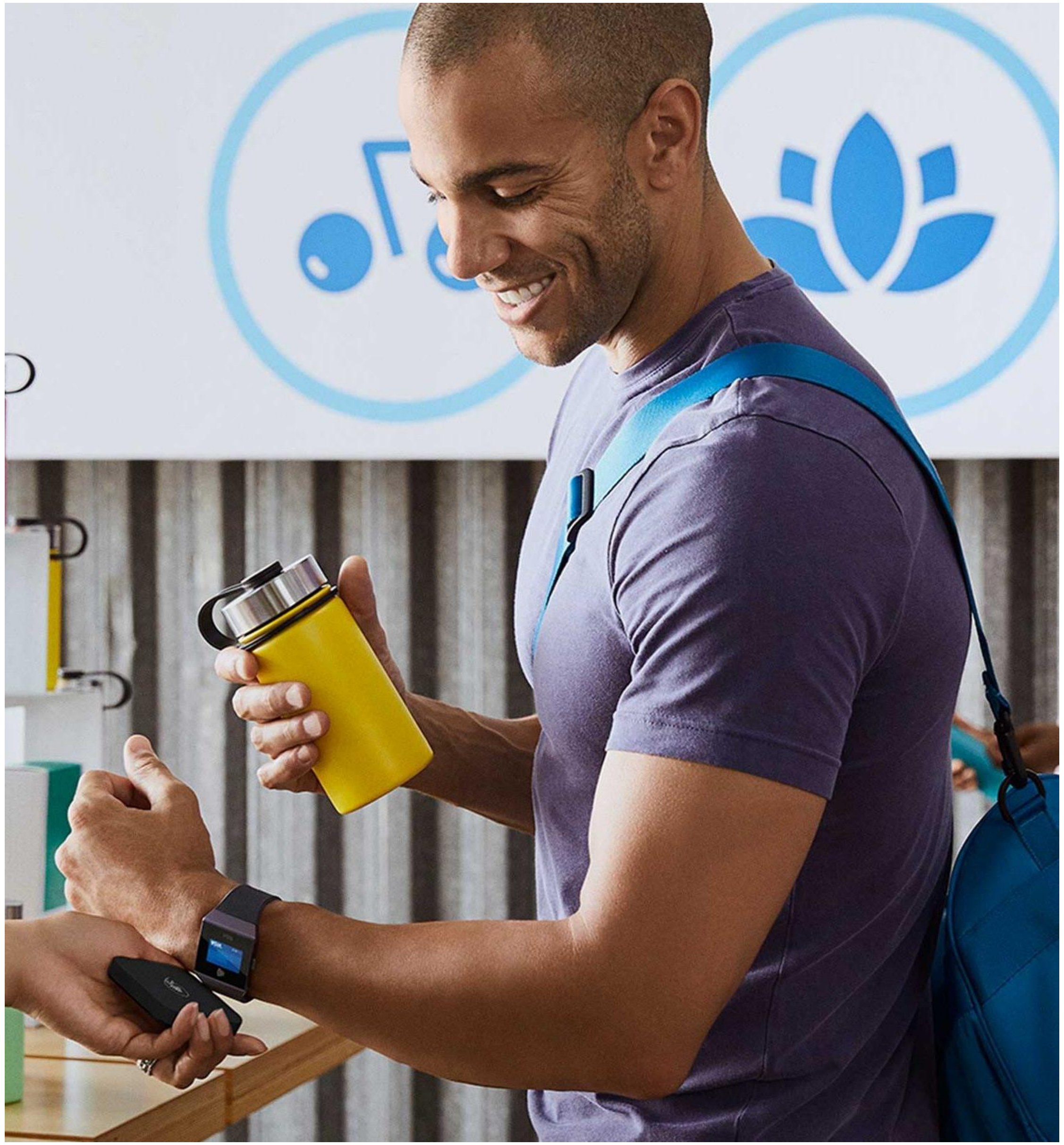
Digital Bank is an example Bank created to demonstrate the authentication process only.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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 (X)* consecutive contactless purchases without providing authentication or;
- The cumulative value of contactless payments since the last time authentication was provided exceeds (Y)* in total or;
- An Issuer wishes to verify the customer.



*Depends on local regulations requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Implementing SCA

3.1 Speaking to your Acquiring partner

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 Acquiring partner:

- 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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.2 Implementation for online businesses

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

Contact your Acquiring partner
Once you have implemented 3DS through your Acquiring partner, your Acquiring partner 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 your customers using **3-D Secure (3DS)** – Visa offers this service via Visa Secure. Without Visa Secure your customers may be unable to complete online transactions.

Support the version 3DS 2.2.0 for the best customer experience especially when selling in-app and on smartphones. It also brings important advantages to your business.

12 April 2024 Visa Secure issuers required to support EMV 3DS 2.2.0.

25 September 2024 Visa will discontinue support for EMV 3DS 2.1.0 transaction processing.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.2 Implementation for online businesses

Response code 1A is a tool for the issuer to inform the merchant that the transaction would be reconsidered for approval if it is re-submitted with authentication data

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

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

If issuer declines requesting authentication (SCA Decline Code 1A), the transaction will need to be submitted via 3DS, with a step-up request: merchant must be ready to handle these "soft declines" by their SCA local laws enforcement date.

Code 1A

Response code 1A – Additional customer authentication is required

Merchants will need to be able to respond to an SCA decline code by

- Resubmitting the transaction via EMV 3DSwith the 3DS Requestor Challenge Indicator set to 04 (Challenge Requested: Mandate) to ensure that SCA is applied.
- Resubmitting the transaction to authorization with the CAVV and ECI values received

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.3 Implementation for in-store 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 Acquiring partner processes a transaction, they send your business a 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 (X)* consecutive contactless purchases without providing authentication or;
- The cumulative value of contactless payments since the last time additional authentication was provided exceeds (Y)* in total or;
- An Issuer wishes to verify the customer.

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

Code 70

Response code 70 – this applies to ask the customer to enter their PIN.

Code 1A

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

Contact your Acquiring partner

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

*Depends on local laws requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.4 Take advantage of exemptions*

Contact your Acquiring partner

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 **online** payments**.

- **Low value payments online.** Payments below (X)** are exempt from SCA. (However, the customer`s bank may request authentication.)
- **Low-risk online payments.** As part of the new security measures, banks may be able to make better and faster risk analysis decisions as they will be provided with more extensive data. SCA can be not required if an online payment is determined to be low risk using real-time transaction analysis.
- **Trusted merchants.** Cardholders can be able 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.

* List of exemptions depends on local regulations
** Depends on local regulations requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.4 Take advantage of exemptions*

Contact your Acquiring partner

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 pass two-factor authentication to make in-store payments.**

- **For contactless payments under (X)****
  (However, after (Y)** consecutive transactions, or if cumulative value of contactless payments since the last time authentication was provided exceeds (Z)**, Issuer still may request customer authentication via authorization response code.)
- **Unattended transport and parking terminals.**
  Any payment for transport fares or parking fees at unattended terminals (e.g. at an airport or train station) will not require SCA**.

* List of exemptions depends on local regulations
** Depends on local regulations requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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 and depends on local laws.

Important for merchant*:
Know when to apply SCA
Correctly flag out of scope transactions

- **Merchant Initiated Transactions (MIT).** These include subscriptions and installments 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 at your Merchant on a card issued outside your country.** Note that in these cases, SCA should still be applied on a 'best effort' basis (where it is possible) so SCA may be performed.
- **Anonymous transactions.** SCA may not be needed if customers make a purchase with an anonymous prepaid card.

* PSD2 SCA for Remote Electronic Transactions Implementation Guide February 2023 (Version 4.0) as can be modified by Visa from time to time

VISA

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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 and depends on local laws.

Important for merchant*:
Know when to apply SCA
Correctly flag out of scope transactions

Merchant Initiated Transactions (MIT)

Use correct/appropriate MIT indicators - merchants and their acquiring partners must be reminded that when a Merchant-Initiated Transaction (MIT) is performed, it is essential to flagged it as MIT so that issuers can recognize it is out-of-scope. In the Visa authorization system, it is also important that the correct MIT type is used to indicate to the issuer the intention of the transaction. For example, the merchant may not use recurring flags to charge the cardholder a cancellation fee (no show MIT). We encourage merchants to be familiar with the various MIT types as documented in the Implementation Guide*.

Resubmission authorization transaction - resubmissions are a type of transaction which can only be used where the merchant is re-submitting a previously declined authorization due to lack of funds. This can only be used in case of contactless transactions performed in the transit environment and where a service has already been delivered. Resubmissions must not be used in other sectors and for declined authorizations where the services (or goods) have not yet been delivered. In the case of an MIT other than Resubmission being declined (for example a recurring payment), a Resubmission must never be used. Depending on the decline response code, the merchant may later attempt a new authorization request with the same MIT type (recurring in this example), until it is either approved or a maximum retry limit is reached.

* PSD2 SCA for Remote Electronic Transactions Implementation Guide February 2023 (Version 4.0) as can be modified by Visa from time to time

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

3.6 Account verification transactions

There are many reasons why a merchant may perform an account verification (zero value) transaction

SCA required

Setting up an agreement for Merchant-Initiated Transactions*.

Storing credentials on file for the first time for future CITs if Response code 1A received.

SCA is not required

To check the validity and/or expiry date of a payment credential.

* PSD2 SCA for Remote Electronic Transactions Implementation Guide February 2023 (Version 4.0) as can be modified by Visa from time to time

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

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.

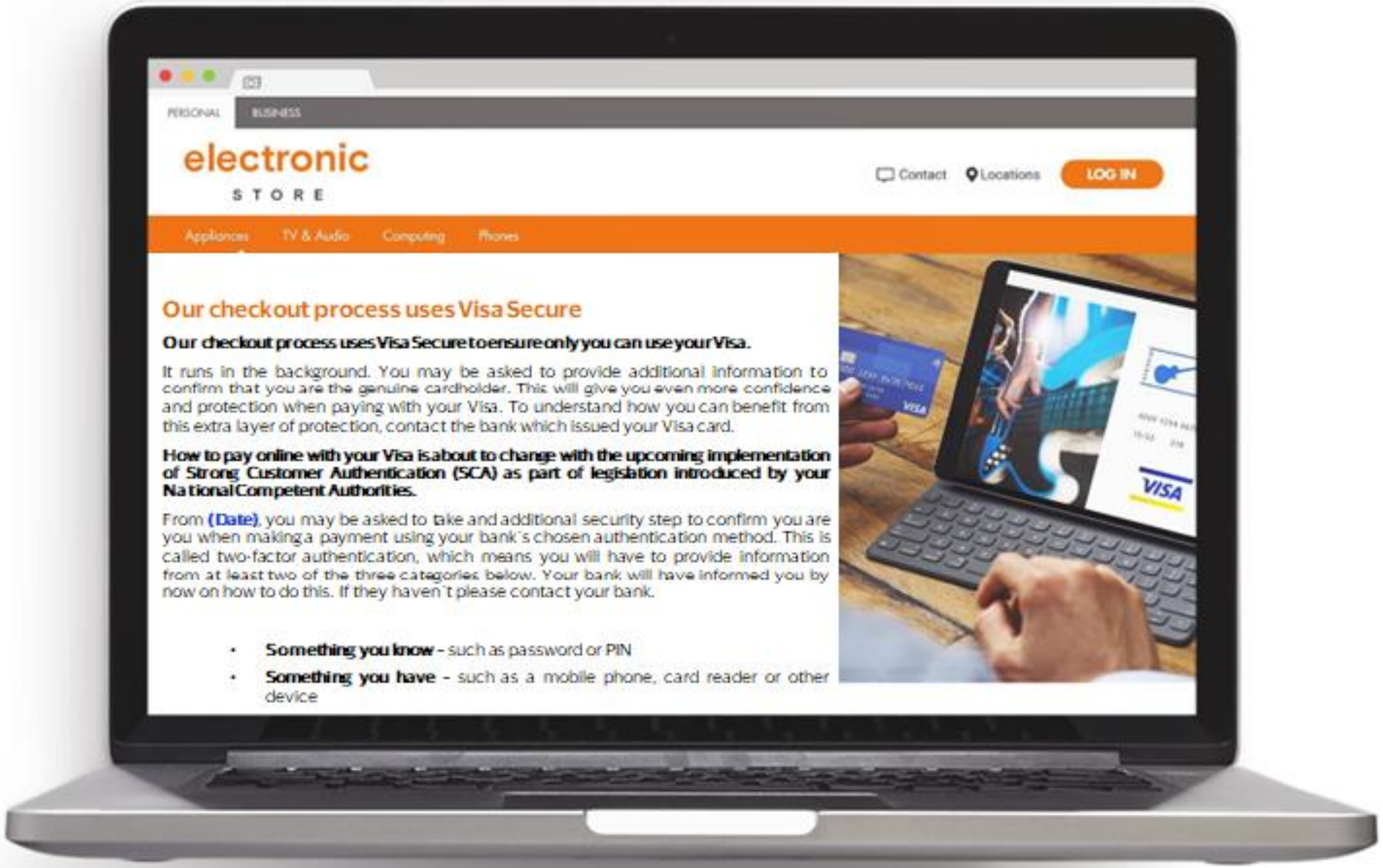
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

4.2 Marketing Communications Guidance for online businesses

4.2.1 Website paragraph

Here’s an example of how you may consider communicating 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 to pay online with your Visa is about to change with the upcoming implementation of Strong Customer Authentication (SCA) as part of legislation introduced by your National Competent Authorities.

From **(Date)**, you may be asked to take and 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.

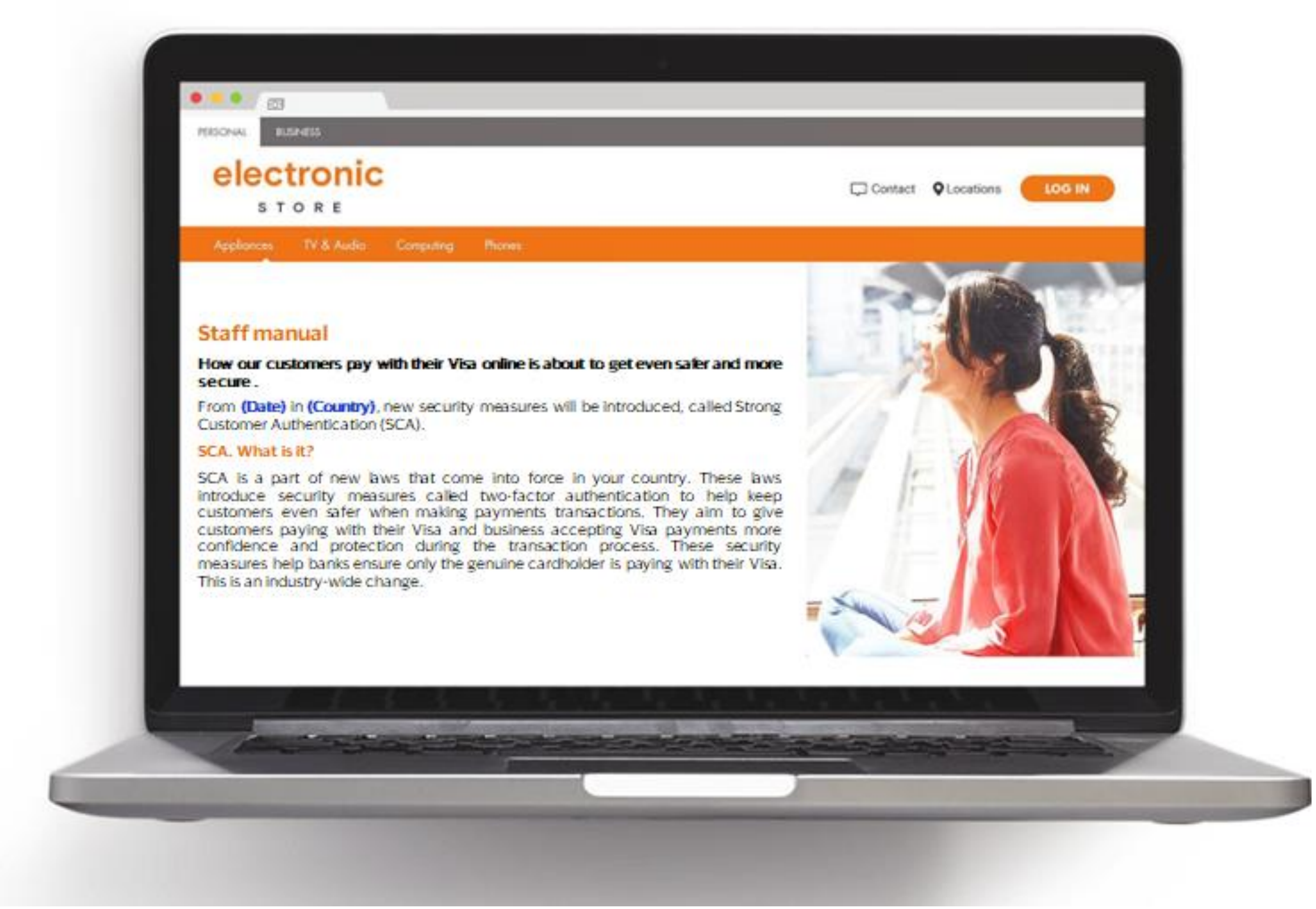
- **Something you know** - such as password or PIN
- **Something you have** - such as a mobile phone, card reader or other device

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

4.2.2 Staff manual

Here's an example of a staff manual which shows how you may consider communicating 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 a part of new laws that come into force in your country. These laws introduce security measures called two-factor authentication to help keep customers even safer when making payments transactions. They aim to give customers paying with their Visa and business 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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

4.2.3 Website call-out

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

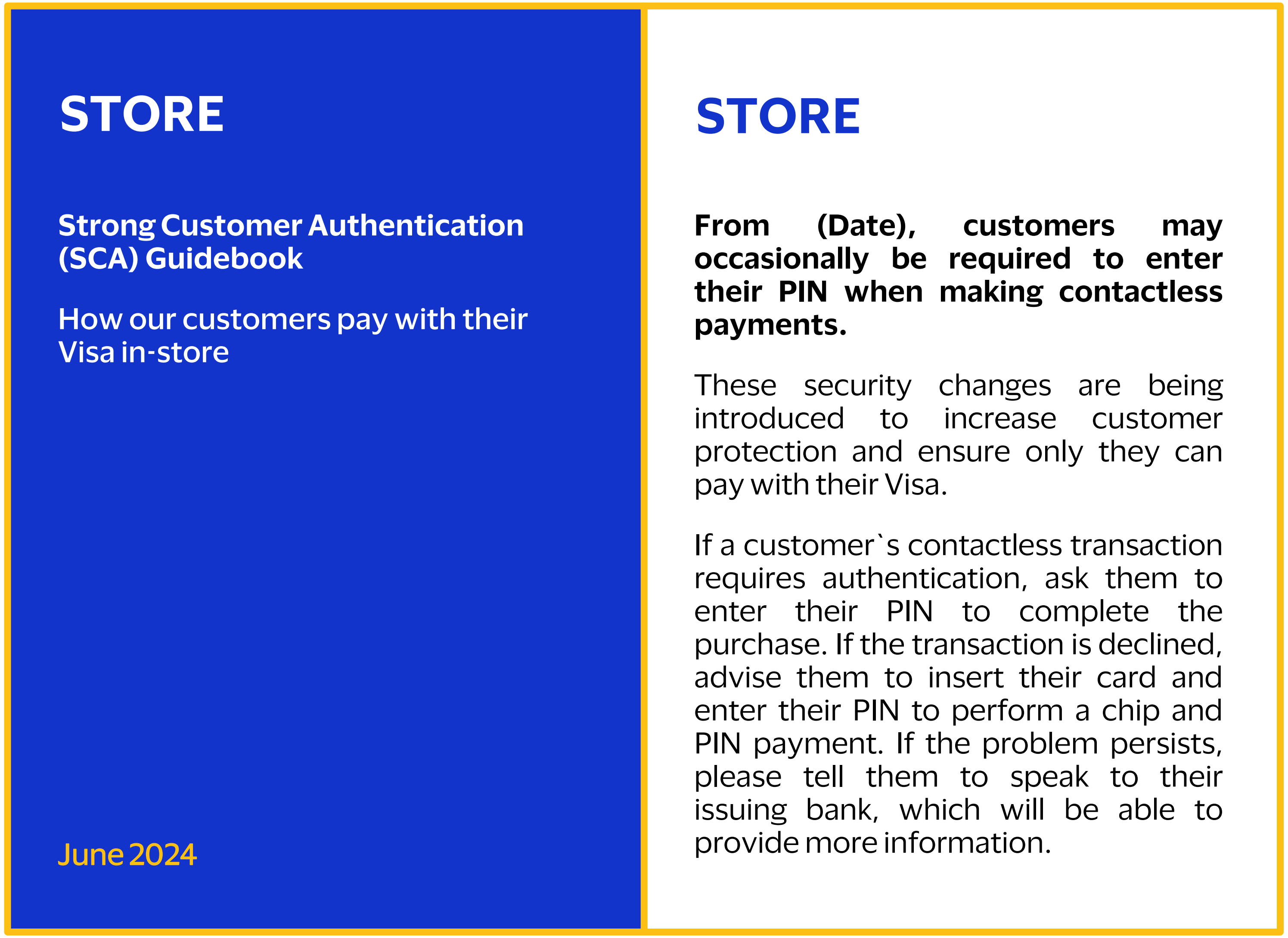
This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

4.3 Marketing Communications Guidance for in-store businesses

4.3.1 Conversation aid

Here's an example of a more concise version of the staff manual. It highlights how you can 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 ›]



STORE

Strong Customer Authentication (SCA) Guidebook

How our customers pay with their Visa in-store

June 2024

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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

4.3.2 Staff manual

Here's an example of how you can 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 Acquiring partner processes a customer transaction, they send a 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 the **(X)*** consecutive contactless purchases without providing authentication or;
- When the cumulative value of contactless payments since the last time additional authentication was provided exceeds **(Y)*** in total or;
- When an Issuer wishes to verify the customer

*Depends on local regulations requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix: Detailed Communications Materials

Here you`ll find some suggested communications for cardholders.
These are the guiding documents that you can use in your messaging.

4.2.1 Website paragraph

Here's an example of how you can 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 card. 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 National Competent Authority.

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 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.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.2.2 Staff manual

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

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 in your country. 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 card, 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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.2.2 Staff manual

Here's an example of a staff manual which shows how you can 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 (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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.2.2 Staff manual

Here's an example of a staff manual which shows how you can 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 in your country 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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.2.2 Staff manual

Here's an example of a staff manual which shows how you can 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.

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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.3.1 Conversation aid

Here's an example of a more concise version of the staff manual and highlights how you can 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 card.

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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.3.2 Staff manual

Here's an example of how you can 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 Acquiring partner processes a customer transaction, they send a 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 (X)* consecutive contactless purchases without providing authentication or;
- When the cumulative value of contactless payments since the last time additional authentication was provided exceeds (Y)* in total or;
- When an Issuer wishes to verify the customer

* Depends on local regulations requirements and Issuer implementation.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.3.2 Staff manual

Here’s an example of how you can 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 – asks the customer to enter their PIN.

2. Response code 1A – 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 in your country. 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.

This material is not legal or other professional advice. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Appendix 4.3.2 Staff manual

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

4. 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. Acquiring partners are responsible for their own compliance with SCA requirements and their own customer communications.
This material must be read together with slide 2.
This guidebook was published in June 2024.

Thank you