Appendix: Detailed Communications Material

Here you’ll find some recommended communications for cardholders. These are guiding documents that you can use in your messaging.

**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.

**Appendix 4.2.1**
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

**Appendix 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 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

**Appendix 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 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.

**Appendix 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 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.

1. **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

\*Insert date as required

**Appendix 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 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.***

1. **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

1. **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.

1. **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.

1. **Is this extra security free?**

Yes. There’s no charge levied by Visa on Merchants for this new layer of protection.

**Appendix 4.3.1**
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

**Appendix 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.*

**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

**Appendix 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.*

***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.

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

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

1. **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

**Appendix 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.*

1. **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.

1. **How does Visa protect customers?**

They’ll be protected by Visa’s zero liability policy if anyone makes a fraudulent transaction with their Visa.

1. **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.**