



Example of Staff manual

This manual provides staff with the information they need to answer common customer questions and provide an understanding of how to inform customers about SCA



IMPORTANT INFORMATION:

The information in this document is provided "as is" and intended for informational purposes only; it should not be relied upon for operational, marketing, legal, technical, financial, tax, or other advice. You should consult your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits to be realized as a result of implementing any recommendations or programs may vary based on your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results, and they are subject to risks, uncertainties, and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy, or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by local law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including without limitation, any special, indirect, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary losses, even if advised of the possibility of such damages.

As a new regulatory framework in the evolutionary ecosystem, SCA requirements still need to be clarified for some use cases. This document represents the evolution of Visa's thinking, but it should not be considered as a final position or as legal advice, and it is subject to change in accordance with guidance and clarifications of the competent authorities. Visa reserves the right to revise this document pending further regulatory developments.

New security measures are being implemented – Strong Customer Authentication (SCA).

What is it?

The SCA is part of new laws that have entered into force in your country. These laws introduce security measures called Strong Customer Authentication to help keep customers even safer when making online payment transactions. The new changes are aimed at improving security and fraud protection for customers and businesses when making payments with Visa. This is an industry-wide change.

How does it work when you buy from us?

When customers pay with their Visa cards, they may be asked to take an additional security step to verify their identity using an authentication method chosen by the bank. This is called two-factor authentication, which means that the customer will need to provide information from at least two different categories, listed below:

Knowledge – for example, password;

Possession – for example, mobile phone or other device;

Inherence – for example, iris scan, facial recognition or fingerprint.

How will customers set up new subscriptions or recurring payments?

When setting up an agreement for a new subscription, the customer may need to confirm their identity using two-factor authentication selected by the bank. At the same time, all subsequent subscription payments will not require two-factor authentication. Authentication may be required if the customer wants to make changes to their subscription agreement.

What does SCA mean for our customers?

From (date), the user experience, our customers get when purchasing online, may change due to two-factor authentication. The enhanced level of security will help customers strengthen trust and confidence when shopping online. Customers will be able to pay using a variety of devices, such as smartphones, tablets and laptops, which will improve the user experience.

As part of the changes, banks will have more data to make informed decisions and evaluate transactions: low-risk transactions (SCA exemptions) or out of scope transactions. This will help create a more seamless payment process, reducing the risk of fraud and the number of times cardholders need to authenticate their payments.

What do we need to do?

We all need to be informed about the changes that SCA will bring to raise awareness and help our customers. However, if they have questions that you cannot answer, please refer to the Issuing Bank that can provide more information.

How will the response codes change?

A new response code may be applied during the transaction process.

Currently, when our acquiring partner processes a customer transaction, it sends a response code from the issuing bank to indicate whether the payment was approved, declined, or what the next steps are. A new response code will be added once SCA is implemented.

Response code

Banks control the new response code.

For our business to be ready by **(date)**, we need to make sure we support these new codes

Response code 1A - additional client authentication required

Response code 70 - PIN data required.

Questions and answers

1. What is SCA?

From (date), banks are implementing new security measures within the framework of the new laws that have come into force in your country when paying by cards. This makes paying with Visa even more secure with two-factor authentication, which provides an additional level of security when making online payments. This will help banks get confirmation that only the genuine cardholder is using the Visa card.

2. How will our customers pay online when the SCA comes into force?

Customers may be prompted for an additional security step to verify their identity using the authentication method chosen by the bank. They must provide information from at least two different categories below:

- 1. Something the customer knows**
for example, a password.
- 2. Something the customer has**
such as a mobile phone or other device.
- 3. Something the client is**
for example, an iris scan, facial recognition or fingerprint.

3. What should our customers do if their transaction is declined or they don't know how to authenticate?

Advise customers to contact their bank. The issuing bank will be able to provide the client with more detailed information.

4. What is Visa Secure?

Visa Secure is a technology that banks use to ensure enhanced security of our customers' payments in the online environment. When our customers see 'Visa Secure', they can be sure that their transaction is protected by multiple levels of security.

5. Is this extra security free?

Yes. Visa does not charge merchants any fees or commissions for this new level of protection.