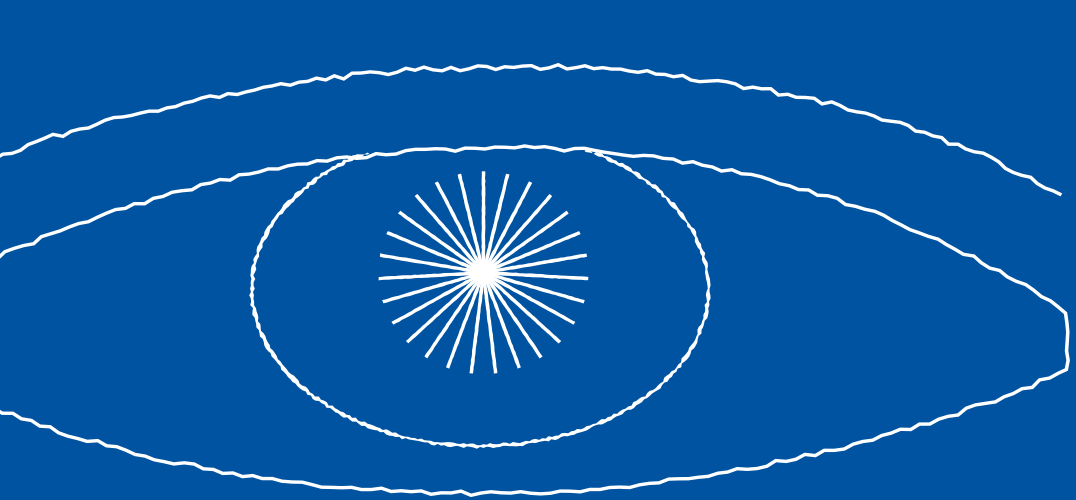
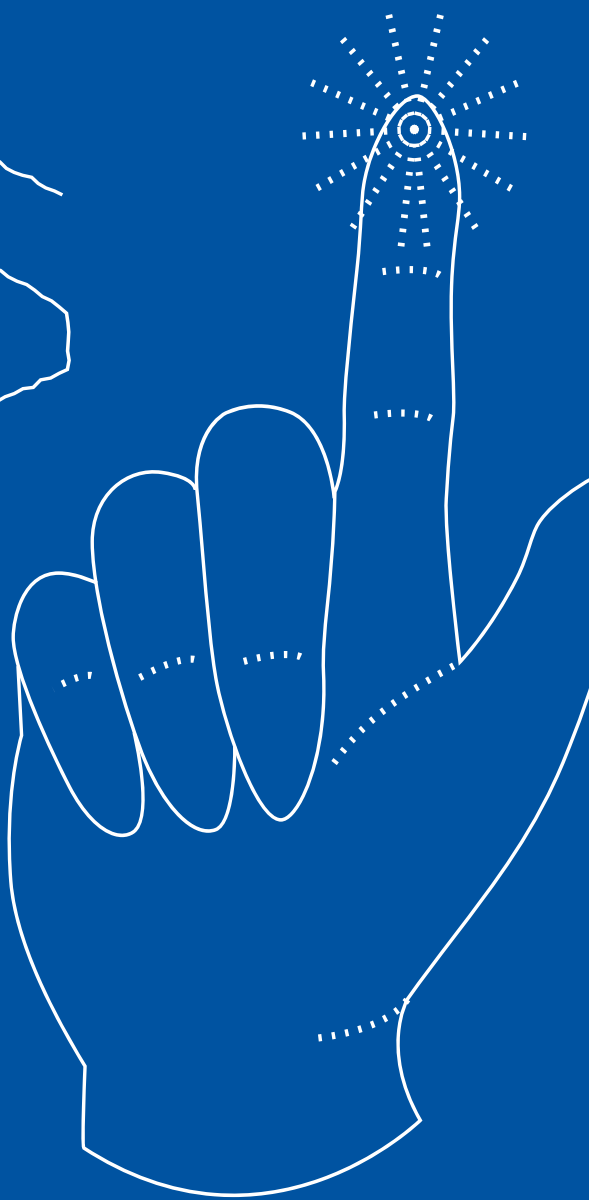
A complete guide to SCA

Strong Customer Authentication





GOCARDLESS

01.
An introduction to Strong Customer Authentication

The background to PSD2 and SCA

The PSD2 is the 2nd EU Payments Service Directive.

The directive builds on three key areas of legislation first brought in with the original 2007 Directive. These areas include increased consumer rights in payments, creating a level playing field by bringing into scope the regulation of third-party access to account information and enhanced security.

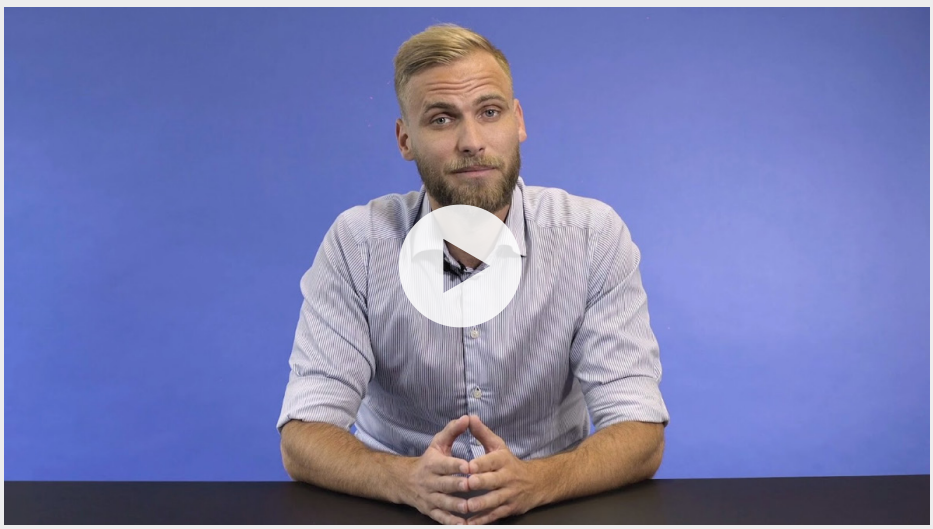
Enhanced security refers specifically to a set of requirements called **Strong Customer Authentication (SCA)**. These requirements have far-reaching implications for any business with an online presence.

This guide will explore SCA, who and what it affects and how businesses can prepare for the requirements taking effect.

What is Strong Customer Authentication (SCA)?

Strong Customer Authentication is a set of upcoming regulatory requirements, designed to make paying online more secure and, consequently, reduce payment fraud.

SCA adds an extra layer of security when end-customers make a payment online. Until now, shoppers have been able to simply enter their payment details and complete their purchase (although some businesses voluntarily choose to ask for further authentication).



How does SCA work?

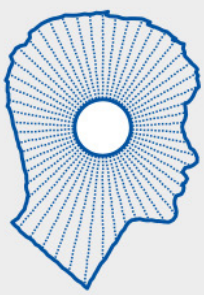
SCA is a form of two-factor authentication designed to prove that end-customers are who they say they are, with specific rules around what constitutes 'authentication'.

It requires two forms of validation out of three available categories.

What constitutes a method of authentication?

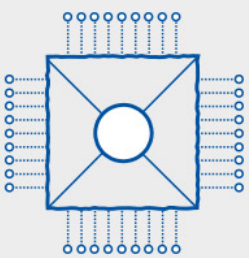
There are three valid categories of authentication available as part of SCA. Within each category, there are a number of potential methods for satisfying that category.

The three categories are:



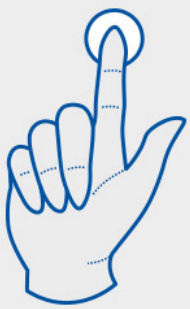
Knowledge

Something you know, e.g:
Password
PIN



Possession

Something you possess, e.g:
Mobile phone
Smart watch



Inherence

Something you are, e.g:
Fingerprint
Facial recognition

Only when the payer has been able to provide two of these forms of authentication, will they be allowed to complete their payment.

On 21 June 2019, the EBA released a new opinion on what may constitute a compliant element in each of the three possible categories of inherence, possession and knowledge, as well as additional requirements on dynamic linking and the independence of elements.

What transactions does SCA apply to?

SCA is being brought in to make dealing with money and making payments online more secure and to reduce payment fraud. At a high level, SCA will be required where a payer transfers funds or access their account information.

In particular, SCA applies each time a payer:

- accesses its payment account online
- initiates an electronic payment transaction
- carries out any action through a remote channel which may imply a risk of payment fraud or other abuse

The main impact is very likely to be on card payments and bank transfers. The reason for this being that card payments are instant and initiated by the end-customer, and the payment or the consent to access account details is instant, which creates risk.

Does SCA apply to recurring payments?

Where payments are initiated by an end customer, SCA will only apply to the first payment in a set of recurring payments for the same amount. However, if the amount changes, then SCA will apply.

Where payments are initiated by the merchant receiving the funds, SCA will typically (although not in the case of standard Direct Debits) be required for the first payment in a series of recurring payments. So long as the subsequent payments are initiated by the merchant, further SCA will not be required so long as the amounts being charged are within the reasonable expectation of the end customer.

This means subscription businesses, SaaS businesses and membership businesses will all need to prepare for SCA.

There are, however, multiple exemptions to SCA, and certain out of scope transactions that will benefit businesses with recurring revenue.

Why is SCA coming into force?

SCA is part of PSD2. One of the aims of PSD2 is to provide protection for consumers.

Since the implementation of the original PSD, there have been new technological advances within the payments market seeing an increase of Third Party Providers (TPPs). These TPPs offer new and innovative ways of accessing consumers' account information and initiating payments.

However, opening up access to consumer accounts in this way creates increased security risk, and the tradeoff is strict regulation on how TPPs and payment service providers get access to these accounts.

That's where SCA comes in. It aims to ensure that the end customer is the rightful owner of the bank account or other payment mechanism (e.g. card). By going through a two-factor authentication process, the risk of fraud is perceived to be reduced.

In short, SCA is aimed at improving the security of payers' online transactions and reducing payer fraud.

The cost of payments fraud

SCA is designed to reduce fraud during online transactions, but how much impact will it make?

Europol estimated that card-not-present fraud accounted for 66% of €1.44 billion in fraudulent card transactions in 2013. By 2016, the European Central Bank (ECB) calculated the total cost of card payment fraud reached €1.8 billion. The UK, France and Denmark suffered from the highest rates of card fraud.

In the UK alone, £2 billion was stolen from credit and debit cards in 2017, with 28% of people becoming the victim of online payment fraud.

Any reduction in the rate of fraud could result in a significant saving across Europe.

What countries will SCA apply to?

SCA (as part of PSD2) is a European-wide requirement and will be required for any applicable transaction where both the business' payment service provider and the payer's bank or card provider are located within the European Economic Area (EEA). If one of these is outside Europe, the requirement is for the payment service provider in Europe to use 'best efforts' to apply SCA.

This means that even if a business is headquartered outside the EEA, if they take online payments from payers in the EEA, those transactions may still be subject to SCA.

It is highly likely that SCA will continue to apply to the UK, regardless of the outcome or timing of Brexit; the FCA has made its plans clear - it wants SCA to continue to apply; there has been no suggestion to the contrary by other European regulators.

The European Banking Authority's role in SCA

The European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.

The EBA has released Regulatory Technical Standards (RTS) that outline the full remit of SCA for the EEA.

However, competent authorities from individual EEA countries, such as the FCA in the UK or BaFin in Germany will be responsible for enforcing SCA when it comes into force.

When does SCA take effect?

SCA is currently planned to come into force across the European Economic Area from 14 September 2019.

Note: The FCA released a statement on 28 June 2019 recognising concerns around the industry's preparedness and ability to comply with the requirements for SCA by 14 September 2019.

This means that some PSPs may be allowed a delayed roll out, otherwise known as an 'operational readiness' period, during which the FCA and other regulators may not take enforcement action.

The overall timeline for any delayed roll out is still being finalised, but it has been suggested it will last approximately 18 months from September 2019 - the initial planned date for the new requirements coming into force.

02.
Preparing your business for SCA

How ready for SCA are online businesses?

In 2018, Mastercard surveyed over 300 online merchants and found that 86% of those were not yet SCA compliant, while 75% weren't even aware of the upcoming legislation.

A May 2019 study by 451 Research found that only 15% of businesses feel 'extremely prepared'. While many of those who admit to being unprepared are small businesses, the readiness problem is more widespread. According to the research, only 19% of businesses with more than 5000 employees feel extremely prepared, and only two in five businesses anticipate being SCA compliant prior to September 2019.

There are, at least, indications that online businesses are starting to take note - SCA was a major topic of conversation at fintech and payments events such as Merchant Risk Council London 2019 and Money 20/20.

The potential business impact of SCA

While more businesses are starting to wake up to the impending SCA legislation taking effect in September, many are still considering what the potential effects of SCA will be. Here are four potential impacts of SCA.

1 Conversion rate drop off

For transactions that require authentication, the new legislation means additional steps during the checkout flow. Friction during checkout can greatly increase the likelihood of a potential end customer not completing a purchase. 69% of purchases were abandoned in 2019 and 27% of those who did abandon a purchase did so because the process was 'too long or complicated'.

While there are exemptions available for certain types of transactions and other general tactics that businesses can implement to reduce checkout friction, SCA will likely result in reduced conversion rates for businesses unable to balance the new security measures with a convenient checkout experience for end customers.

In India, similar legislation saw an 'overnight' conversion rate drop of 25% across all affected businesses.

2 The economic impact of SCA

The result of fewer end customers completing purchases due to the new authentication process is expected to have a knock-on effect on the European economy. European businesses stand to lose an estimated €57 billion in the first year after SCA implementation.

3 End customer reimbursements

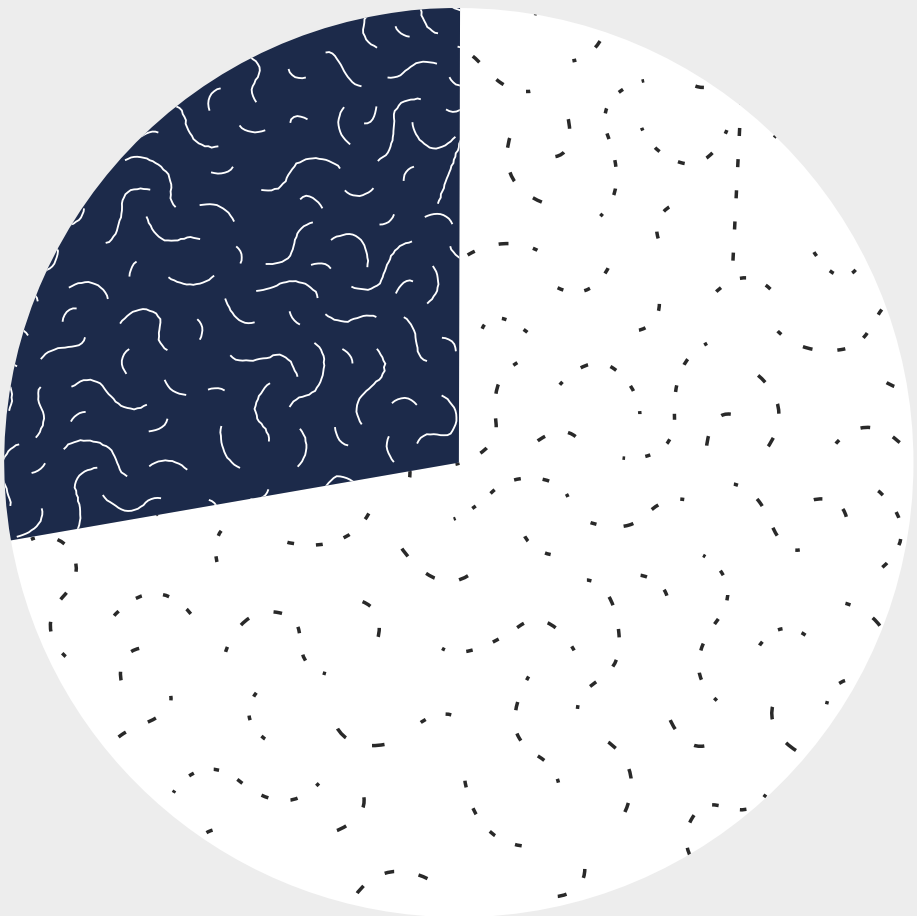
According to the European Payments Council: "PSD2 foresees that the payer can claim full reimbursement from their PSP in case of an unauthorised payment if there was no SCA measure in place and if the payer did not act fraudulently."

In practice, this means that where a merchant's PSP (e.g. a card acquirer) chooses to either rely on an exemption (to not apply SCA) or does not implement SCA at all, they will be liable for any resulting fraud. Where SCA is applied, that liability can be shifted to the party applying SCA - that is, the payer's PSP (e.g. the card issuer). Where a merchant forces its PSP (e.g. a card acquirer) to apply a specific exemption, there is nothing preventing the PSP and merchant agreeing where liability ultimately sits, and we expect that liability to be passed to the merchant themselves.

Card networks such as Visa have been hard at work updating their rules to reflect these liability provisions.

4 Demand on resources

In the short term, becoming SCA compliant will require product, legal, operations and finance teams in affected businesses to help implement changes. If merchants choose to communicate changes to end customers, it will also require marketing effort for messaging to resonate in the best possible way.



71% of businesses believe the resource burden for implementing SCA is 'significant'.

How to implement SCA

Who is responsible for implementing SCA?

Businesses taking online payments are not directly responsible for meeting SCA. That responsibility falls to intermediary Payment Service Providers (assuming relevant online transactions fall under that provider's remit) and to the banks.

To be more precise, the payer's bank is responsible for ensuring transactions are SCA compliant (and denying transactions that aren't compliant). To do that, it must collect the authentication information as prescribed in the SCA framework.

However, the bank needs somewhere to collect that information from, which is where the PSPs come in. They must capture the information securely, as part of the payment flow, and then securely pass that information on to the banks using the banks' secure mechanisms for doing so. The banks then have the final say on whether that particular transaction is compliant.

Whilst it is the responsibility of the PSP to apply SCA, there can be practical difficulties given the degree of control one PSP may have over the activities or compliance of another PSP.

Ultimately, each PSP has to ensure its own compliance which could, in some cases, lead to a more draconian approach being taken to SCA by a payer's PSPs than has necessarily happened in the past.

However, the impact of SCA that we have already outlined, including potential conversion drop offs, primarily falls on the shoulders of merchants.

Working with a PSP that is either prepared and proactive about SCA will be critical.

If you want to talk in more detail about SCA and the implications for your payments, we'd be happy to chat.

Updating your checkout flow

The process of complying with SCA means an extra step during the checkout flow. This will be the most obvious change your end customers will see. Depending on the payment method, this additional step may be very obvious or almost unnoticeable. For example, mobile payments already use fingerprint scanning or facial recognition to approve purchases, and these are acceptable 'inherence' authentication measures.

As we have already mentioned, SCA will primarily affect credit and debit card transactions. To update your checkout flows for card transactions, 3D Secure 2 (3DS2) - a widely supported method of compliant authentication has already been released.

In a recent article for Forbes, Jordan Mckee, Research Director at 451 Research pointed out that "merchants best able to integrate SCA into their checkout flow and effectively apply exemptions will separate themselves from the pack by minimizing customer impact."

3D Secure 2

3D Secure (3DS) is a method of authentication first deployed by Visa, made for credit and debit card purchases completed online. End customers are required to provide a password in order to complete the payment transaction. Online businesses typically gain access to 3D Secure through a relevant PSP.

3D Secure 2 (3DS2) is a new version that will meet SCA requirements by introducing authentication requirements, e.g. requiring end customers to input a one-time password/passcode or provide biometric authorisation.

However, testing and rollout by all parties is unlikely to be fully finalised by 14 September.

The key goal for 3DS2 is to create 'frictionless authorisation' even in the face of additional security checks required by SCA. If the transaction is deemed exempt, 3D Secure 2 should bypass these checks. One key improvement compared to the original 3D Secure (3DS) protocol is the ability to carry out the necessary checks without redirecting away from the checkout page.

Potential problems of 3D Secure 2
The original 3D Secure (3DS) was fraught with problems for merchants, including the dreaded conversion drop because of the aforementioned redirects and perceived poor user experience. A study by Ravelin found that 22% of all transaction authenticated using 3D Secure are lost.

While the new version has been designed to minimise the original's drawbacks, including a better user experience designed for smartphone users, it will require a wider rollout to evaluate whether it has been successful.

3DS2 support and consumer recognition
3D secure 2's success in managing SCA conversion concerns will hinge on its adoption by both banks and end customers. Despite the impending implementation of SCA, a number of banks have yet to start supporting the 3DS2 protocol.

As for end customers, usage of the original 3DS protocol has been limited in Europe. According to PYMNTS, by late 2017, only 50% of end customers are enrolled and only 25% of transactions are verified.

SCA Regulatory Technical Standards (RTS)

The Regulatory Technical Standards (RTS) of SCA set out the full specifications of exactly what SCA covers and what is expected of all stakeholders. The final version was completed and distributed by the EU Commission in November 2018.

Your customers and SCA

While SCA will undoubtedly have an impact on your business, it will also be a noticeable change for end customers trying to make purchases online. How do they feel about it? Do they even care about added security? Do they know the changes are coming?

Banks have begun to communicate SCA to businesses (example 1, example 2), but have yet to really communicate the changes to the end consumer.

Balancing security and convenience

Regardless of awareness, will end customers be willing to lose some of the convenience of online shopping to accommodate the more extensive security checks of SCA? After all, Amazon's 1-click ordering system was the convenient process that all other checkouts are compared to.

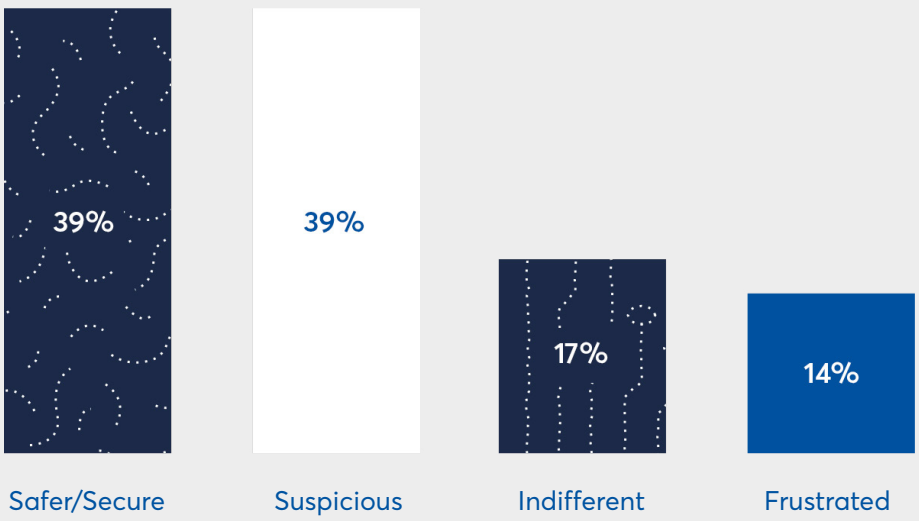
In a study of 4,000 customers across the UK, France, Germany and Spain were asked about their attitudes to both security and convenience when shopping online.

The survey also asked them questions on feelings about certain specific elements of the new SCA requirements, and how increased security at checkout would influence their buying behaviour.

The results uncovered a slight preference for security over conversion, with 58% of shoppers prioritising security.

However, when asked how they would feel if faced with complex security procedures when shopping only, the majority (54%) said they would feel either suspicious or frustrated. Only 39% said they would feel safer.

How would complex security processes make you feel?

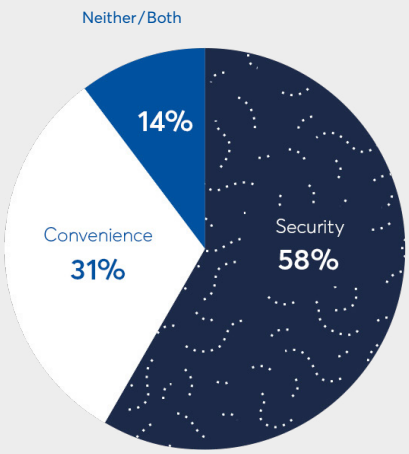


Survey of 4,000 online shoppers in the UK, France, Germany and Spain

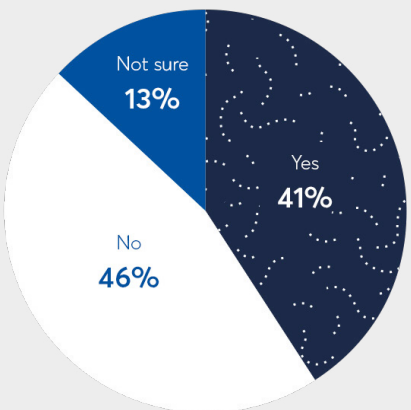
The survey also showed that attitudes to security and actual buying behaviour may be very different. 41% of those surveyed had previously abandoned an online purchase that was too complex, and nearly a quarter (24%) would go as far as to shop less with their favourite brand if the purchase involved added security measures.

This dissonance in attitudes suggests that what end customers think and how they act are different. They may react positively to the idea of added security, but their actual behaviour, when confronted with SCA, could be very different.

What is most important when paying online?



Have you ever abandoned a purchase because of complex security processes?



Survey of 4,000 online shoppers in the UK, France, Germany and Spain

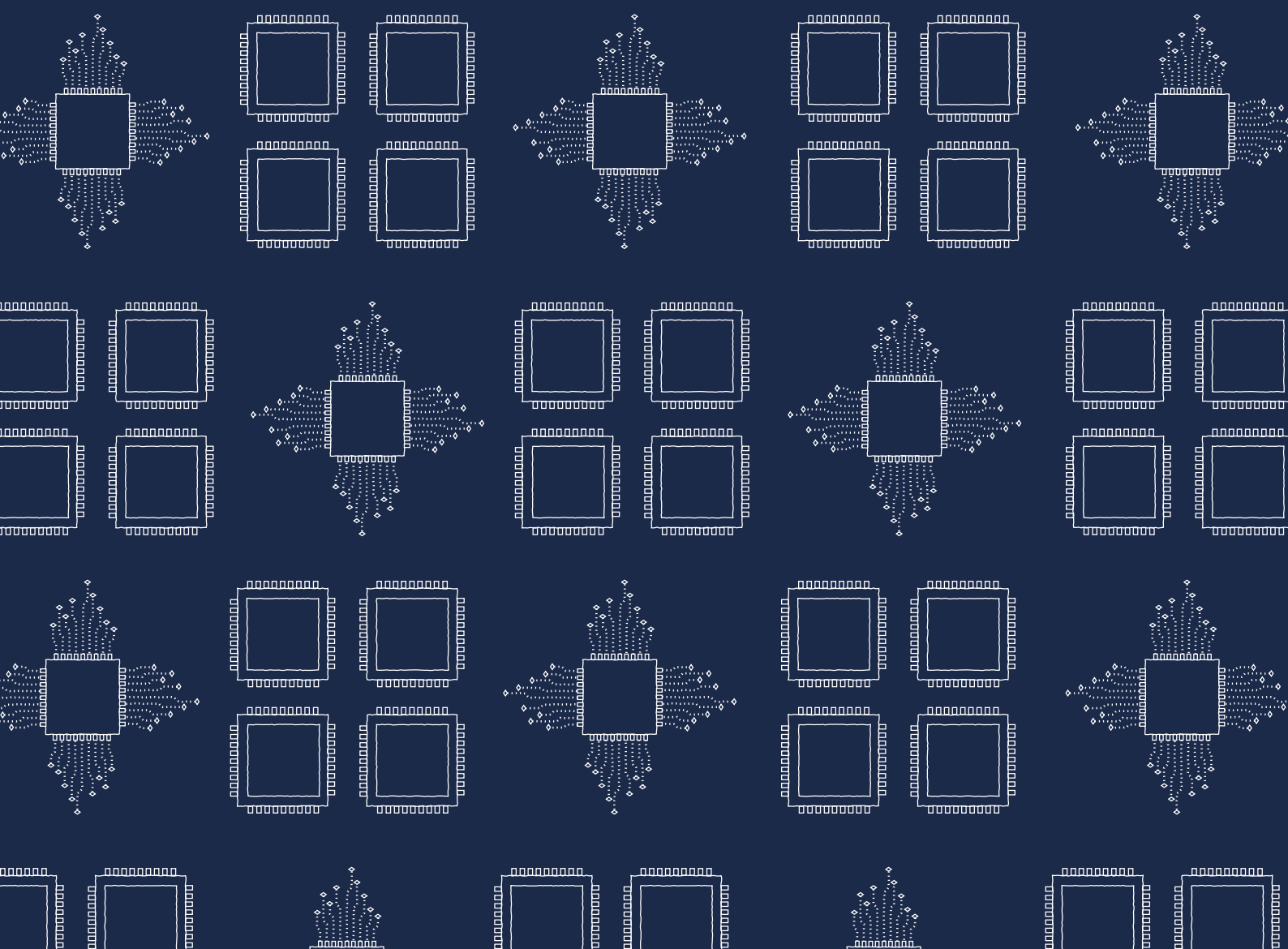
Communicating SCA to your end customers

In the wake of 2018's GDPR legislation, many end customers saw a barrage of emails from companies informing them of changes to privacy policies. The combined effect was poorly received by end customers and many of the emails were even illegal under GDPR.

The point here is that communicating any major changes to your end customers is fraught with its own set of problems. If you don't communicate these changes, will they be confused when changes do take effect? If you do communicate SCA, will this create unnecessary concern? It's also very difficult to communicate the exact nature of any changes when you're still in the process of implementing new checkout flows and authorisation processes.

03.
Exemptions to SCA

Key exemptions and out of scope transactions



Are merchant-initiated transactions exempt from SCA?

Merchant-initiated transactions are classed as out of scope of SCA requirements, so do not need to be 'exempted'. A merchant-initiated transaction is a payment that is taken on an agreed upon date with the payer's consent, and, as the name suggests, is initiated by the merchant collecting the payment.

If a transaction is merchant initiated, both fixed and variable payments will be exempt from SCA.

Unlike most transactions initiated by end customers, the payment flows of merchant-initiated transactions are frequently not instant. The end customer's details are collected at one point in time and submitted to the end customer's bank at another point in time. As such, the communication between the end customer, bank and payment provider does not happen in real-time. In SCA parlance, this is known as an asynchronous transaction. It would be impractical, and in some cases, impossible for SCA to be applied to these transactions.

However, note that for most merchant-initiated transactions, such as recurring card transactions, SCA will still need to be applied to the first payment if that is done with the involvement of the payer's PSP (e.g.a card issuer).

Does that include Electronic 'paperless' Direct Debit mandates?

One type of merchant-initiated transactions are electronic 'paperless' Direct Debits. In order to collect Direct Debits, a 'mandate' must be provided by the end customer from whom payments will be collected, to the merchant/PSP collecting those payments.

There has been a great deal of confusion as to whether SCA is required at the point of setup of the mandate by the payer - specifically, whether the action of setting up the mandate is an "action through a remote channel which may imply a risk of payment fraud or other abuses".

On 7 June 2019, the EBA confirmed via its Q&A tool that Strong Customer Authentication ('SCA') is not required for the set up of electronic 'paperless' Direct Debit mandates provided in favour of merchant payees, so long as the end customer's PSP (e.g. their bank) is not directly involved in that setup.

Specifically, the EBA confirmed:

"Mandates given by the payer to the payee set up without the direct involvement of the payer's PSP are not subject to SCA."

SCA exemptions

While merchant-initiated transactions are considered out of scope for SCA, there are a number of other exemptions that may be relevant to your business.

SCA exemptions only apply to payment service providers. They relate to payment transaction amount, risk of the payment, recurrence of the payment transaction and the payment channel used for execution of the payment. They include:

Fixed recurring transactions and subscriptions

When using a payer-initiated payment method, such as standing orders, only the first payment of a fixed subscription will require SCA. As long as the amount paid stays the same, further transactions will not require SCA.

However, should the amount change, which many usage-based subscriptions do, SCA will be required again for each and every change.

Contactless payments

Contactless payments that meet either of the following conditions will be exempt from the application of SCA:

- Individual contactless payments below €50
- Five or more payments below €50

Where cumulative payments totalling €150 have been made since the last application of SCA, SCA will be required once more.

The exemption is specific to each card used, so for joint accounts, the exemption applies for each card associated with the account.

Transactions below €30

Similar to contactless payments (but with a lower value), payments below €30 will also be exempt from strong customer authentication.

However, SCA will be required if an end customer makes:

- Five or more payments below €30
- If a combination of multiple low value payments totals more than €100

These thresholds are not merchant specific, i.e. those five transactions that add up to €100 or more could be payments to different companies.

Trusted beneficiaries (whitelisting)

Customers will have the option to assign well-known businesses to a list of 'Trusted Beneficiaries'.

This list will be updated and maintained by the ASPSP (Account Servicing Payment Service Provider), who also has authority to remove trusted beneficiaries. A merchant's PSP may build mechanisms to 'suggest' trusted beneficiaries to the ASPSP on behalf of the end customer.

For example, Mastercard hints that as a customer goes through an online checkout flow, at the point of payment setup, there may be a checkbox that requests that the end customer adds the merchant to their ASPSP's trusted beneficiary list. This request will be passed to the ASPSP, who will then require the end customer to go through SCA in order to approve the trusted beneficiary listing. The end customer will also be able to manage their list of trusted beneficiaries direct with their ASPSP.

Note that ASPSPs do not necessarily need to provide the trusted beneficiary list themselves - they can outsource this, and companies such as Visa are developing products as a result.

If a business is on an end customer's 'whitelist' then SCA will not be required, regardless of the amount, frequency or variation of any purchases.

While an appealing way of potentially navigating SCA, uptake of the process by banks has so far been irregular, and there are still many questions as to exactly how it will work in practice. It is suspected that whitelisting won't become a viable tactic until well after September 2019.

It's important to note though, that in addition to whenever a trusted beneficiary is added to an exemption list, SCA must be applied if there are changes made to a trusted beneficiary or if removal of a listing is requested by a merchant's PSP.

3D Secure 2 (version 2.2) will provide whitelisting as an available option to merchants.

Corporate payments

Payments made directly between two corporate companies will be exempt from SCA, but only if the payment method used is a dedicated B2B method e.g. access-controlled corporate travel management or corporate purchasing system.

According to UK Finance: "SCA is not required for payments initiated in respect of legal persons using dedicated payment processes or protocols that are limited to end customers who are not consumers (e.g. host to host, some SWIFT services and some corporate card products)."

The RTS also expands on exactly what will or will not fall under this exemption:

- It expects "the use of proprietary automated host-to-host (machine-to-machine) restricted networks, lodged or virtual corporate cards, such as those used within access-controlled corporate travel management or corporate purchasing system, would potentially be within the scope of this exemption".

- The use of physical corporate cards issued to employees for business expenditure in circumstances where a secure dedicated payment process and protocol is not used (e.g where online purchases are made via a public website) would not fall within the scope of this exemption.

Low risk transaction exemptions

Assuming SCA would normally apply to a transaction, payment providers will have the authority to evaluate transactions and choose not to apply SCA protocols to those deemed as a 'low risk' of fraud.

Payment service providers will be subject to strict thresholds to be granted the ability to evaluate risk rates of transactions in real-time. The payment provider's fraud rates (as a whole - not just for a specific merchant) must be lower than the following thresholds for the specific payment type being used and value of transaction being processed:

Exemption threshold value (i.e. value of payment being processed)	Card based payments*	Credit transfers*
€500	0.01%	0.005%
€250	0.06%	0.01%
€100	0.13%	0.015%

*Fraud Rate must be no greater than these amounts, for the exemption to be applied

Both the payee's PSP and the end customer's PSP (e.g. a card issuer) may apply this exemption (based upon their own overall fraud rates for that payment type).

However, the ASPSP may decide whether or not to accept the application of that exemption. So, for example, a card acquirer (the merchant's PSP) may apply the exemption, but the card issuer may overrule that exemption.

In practice, we expect the merchant's PSP's request to stand, as liability for any resulting fraudulent payment will rest with the PSP that applied the exemption.

Unattended transport and parking terminals

Payment for transport fares or parking fees at an unattended terminal do not require SCA.

Payment account information

Where an end customer uses a TPP providing account information services to access their payment account data, SCA must be applied where that customer is:

- Accessing the balance of a payment account for the first time
- Accessing more sensitive information, such as details of all transactions processed on an account for the first time

However, SCA does not then need to be applied:

- Where the account balance is accessed again
- Where the historical transaction data is accessed within 90 days of the last application of SCA

Credit transfers

For transfers made between (for example) a current account to a savings account, where both accounts are held at the same bank, by the same person, SCA does not need to be applied.

Implementing SCA exemptions

These SCA exemptions will be important in minimising (or even eliminating) the friction caused by the additional authorisation process. But how do you go about making sure these exemptions are actually triggered when a customer is making a purchase?

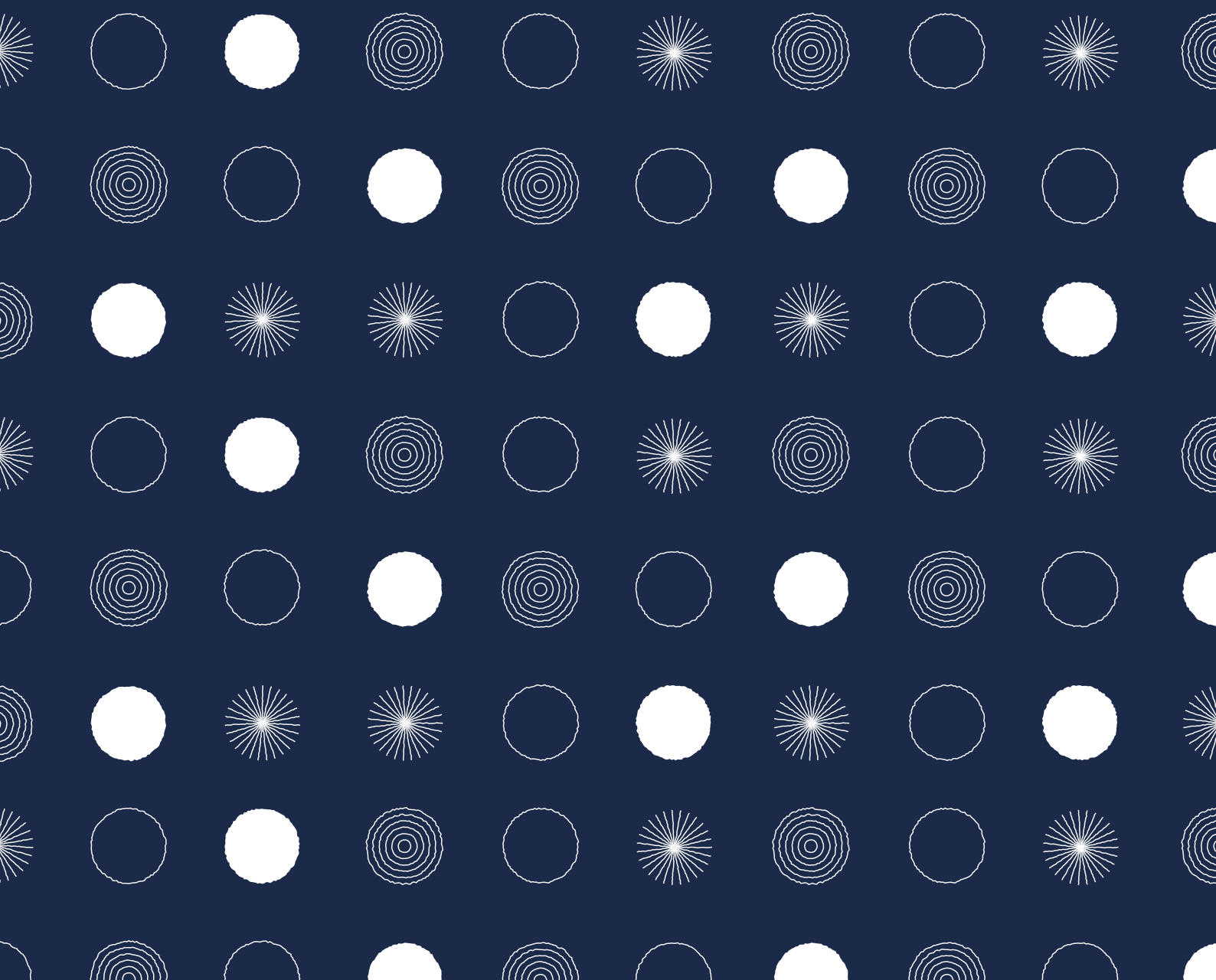
To begin with, it will require PSPs and ASPSPs to work together and to look to utilise common standards e.g. 3DS2.

What if an exemption fails?

While the list of exemptions is now quite clear, the end customer's bank will ultimately decide whether an exemption is valid. If an exemption is not granted, the payment will trigger a decline code. The payment will need to be resubmitted and authorised using Strong Customer Authentication protocols.

04.

Is GoCardless SCA compliant?



Is GoCardless SCA compliant?

GoCardless is fully PSD2 compliant. SCA does not apply to payments through GoCardless.

Our customers will not need to implement any additional authorisation methods for payments collected using GoCardless as a result of SCA.

GoCardless uses 'paperless' Direct Debit mandates, which are out of scope of SCA.

The EBA has also confirmed that the 'paperless' Direct Debit mandates will not require SCA on any payment collection, including any initial payment.

Specifically, the EBA confirmed:

"Mandates given by the payer to the payee set up without the direct involvement of the end customer's PSP are not subject to SCA."

Paperless Direct Debits do not directly involve the end customer's PSP upon setup.

The above confirmation is important to note. Unlike the 'paperless' Direct Debit mandates used by GoCardless, recurring card transactions and 'e-mandates' will require SCA for any initial payment if there is direct involvement from the end customer's PSP upon setup.

Additional protection with the Direct Debit Guarantee

Though not directly related to SCA, it's important to note that the Direct Debit guarantee and indemnity claim protections offered by the Bacs and SEPA Direct Debit payment schemes (and similar protections typically offered for Direct Debit schemes) greatly reduce the risk of payment fraud or other abuses impacting the end customer.

Each offers protection for customers, in that customers are entitled to reverse a payment taken fraudulently or in error, after it has been debited from their bank account.

What do GoCardless customers need to do in preparation for SCA?

For payments collected using GoCardless, no action is needed before or after the 14 September 2019 deadline, because, 'paperless' Direct Debit mandates are not subject to SCA.

However, if GoCardless is only one part of your payment mix, you should consult your other PSPs to see what changes will be required to prepare your other payment methods for SCA requirements.

To find out more about how GoCardless can help your business get ready for life after SCA, talk to one of our payment specialists.

Using GoCardless to build a competitive advantage for SCA

There are several tactics businesses can use to minimise the impact of SCA and protect their conversion rates and revenue. This includes leveraging exemptions and investing in a product like 3DS2 that minimises the friction of two-factor authentication, although these do not completely remove the risk of conversion drop off.

Since payments through GoCardless are out of scope of SCA and fully PSD2 compliant, using GoCardless means you can avoid any potential conversion hit that comes with SCA implementation.

But how else can GoCardless help your business build a competitive advantage post SCA?

Detecting fraud with GoCardless payment intelligence

Direct Debit is a low risk payment method with much lower chargeback rates than cards. We are continuously working to enhance security even further – for example, we are developing a product that will help our customers to detect (and counter) fraud attempts more easily, by applying payment intelligence learned from millions of transactions in our network of more than 40,000 merchants.

Is GoCardless SCA compliant? — page 40

This can be compared to what's called Transaction Risk Analysis in the SCA world, where a merchant is allowed to forego SCA requirements if their payment provider's fraud rate is below a certain threshold.

With this new functionality, GoCardless will analyse every transaction and help merchants spot and stop fraud attempts, without impacting conversion.

The customer preference for Direct Debit

As well as being PSD2 compliant, GoCardless is the preferred payment method for numerous types of recurring payments across Europe.

In a recent YouGov survey of around 12,000 consumers, bank debit/Direct Debit was found to be the most popular payment method in all four purchase types (online subscriptions, instalments, household bills and traditional subscriptions) in all six European markets surveyed (UK, France, Spain, Germany, Denmark and Sweden), plus a number of other international markets.

Additionally, in a GoCardless survey to 4,000 consumers in the UK, France, Spain and Germany, 52% said they were likely or very likely to pay for a subscription by Direct Debit if it meant a smoother checkout.

What is GoCardless?

GoCardless provides a smarter way to take recurring payments from your customers around the globe, eliminating involuntary churn and reducing cost. We already help more than 40,000 businesses get paid on time.

To find out more about how GoCardless can help your business, talk to one of our experts.