Strong Customer Authentication

The State of SCA Adoption in 2021

Fi911™
fintech solutions

Strong Customer Authentication

The State of SCA Adoption in 2021

Fi911™
fintech solutions

Introduction

Security remains a top concern among consumers. This is especially true regarding remote channels like eCommerce; one study commissioned by the European Commission in 2018 found that only 69% of consumers were willing to purchase goods and services online. Among those who avoided eCommerce, 77% (or 24% of total respondents) said that payment security and privacy motivated their decision [1].

This is not an irrational concern. Businesses operating in the eCommerce, airline ticketing, money transfer, and banking services verticals will lose a projected USD$ 48 billion (EUR€39.4 billion) every year by 2023 due to evolving threats and fraudster behaviors. This is a 118% increase over projected losses in 2018 [2].

Governments around the world have taken action in response to these outstanding liabilities. One of the most noteworthy actions taken in the last decade was the introduction of Strong Customer Authentication (SCA) standards as part of the Payment Service Directive (PSD2) in the European Union.

SCA is mainly a concern for merchants and financial institutions operating in the EU. However, those involved in finance outside the continent should stay up-to-date on new developments regarding SCA regulations and other developments as well. Europe is a key market and, although one may presently be able to do business in Europe without complying with SCA standards, that state of affairs may change. Plus, similar regulations could come to other markets.

Our research identified SCA as one of the key factors that will determine the impact of chargeback issuances through 2023 (alongside mobile banking, Visa Claims Resolution, and Mastercard Dispute Resolution).

What is SCA?

Strong Customer Authentication is a formalized set of requirements imposed on businesses as part of the revised Payment Service Directive. It's important to understand a little about this directive before diving into SCA.

PSD2 EXPLAINED

The original Payment Service Directive was put in place to regulate payment services—and payment service providers—across the EU and European Economic Area. The goals were to facilitate pan-European competition, increase consumer protections, and standardize rights and obligations for payment providers and users. Building on the original directive, PSD2 goes further in creating a more integrated and competitive market.

Under the new PSD2 regulations, both Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) are allowed to fill roles previously restricted only to banks. Consumers and businesses operating in the EU will be free to utilize these services. The aim here is to break down barriers to entry for new payment services, thus benefitting consumers by creating a more competitive market.

At the same time, PSD2 also puts more focus on data security as the world continues to transition to a digital economy. It expands overall consumer rights and fraud protections, which is where SCA standards come in.

SCA REQUIREMENTS

In simple terms, SCA rules require an extra layer of authentication during checkout. Limiting verification to card number, address, and CVV is no longer enough. Now, sellers are required to verify the buyer's identity according to at least two of the following three factors:

Possession

Something the user possesses, like a phone or payment card.

Knowledge

Something the user knows, like a 3-D Secure code attached to an account

Inherence

Something the user inherently is, like a fingerprint or other biometric impression.

To illustrate, assume a customer wants to make an online purchase. A merchant operating under SCA standards would be required to verify the user's identity, but they have a few options to choose from in determining how to do so. They may try to verify that:

- ✓ **The customer physically possesses the payment card with CVV verification.**
- ✓ **The customer knows the PIN or 3-D Secure passcode associated with the card.**
- ✓ **The customer can provide a biometric signature connected to the cardholder's account.**

The merchant needs to verify at least two of these three things to the satisfaction of the cardholder's issuing bank. If the merchant is unable to verify a buyer according to those standards, there's a good chance the issuer will simply decline the purchase.

SCA EXEMPTIONS

At this stage in the game, most providers and acquirers should know if SCA standards apply to them or not. These requirements could change from one transaction to the next, based on a number of exemptions to SCA requirements.

The following scenarios are exempt from SCA requirements:

- ✓ Mail order or telephone order payments
- ✓ Transactions involving anonymous prepaid cards
- ✓ One-leg (payer or payee is based outside of the EU) transactions
- ✓ Merchant-Initiated Transactions (MITs), including recurring payments for the same amount to the same merchant
- ✓ Transactions below €30; except in cases when the total amount attempted without SCA exceeds €100
- ✓ Transactions involving a merchant whitelisted by the consumer
- ✓ Secure corporate payments
- ✓ Payments made with lodged cards and virtual card numbers
- ✓ Low-risk transactions

TRANSACTION RISK ANALYSIS (TRA)

The global average transaction value placed via direct traffic in 2019 came to USD $112 (EUR€92) [3]. This means that the majority of transactions would likely fall under SCA requirements, placing a substantial burden on payment service providers (PSPs). Transaction Risk Analysis is a workaround designed to make life easier for these PSPs.

TRA is a method for identifying fraud by observing the behavior of different parties during a transaction that can be deployed in real time to gauge the risk represented by that transaction. TRA is invisible to the customer and adds no friction to the customer journey, while saving time and money for PSPs. To deploy TRA, as opposed to an SCA verification method that could introduce friction to the transaction process, the acquirer in question must demonstrate that fraud is managed and contained. See the chart below for TRA schedules allowed under current rules:

Fraud as a share of total transactions processed over previous 90 days (transaction value, represented in basis points)

TRANSACTION VALUE	CARD-NOT-PRESENT PAYMENTS	CREDIT TRANSFERS
€100	6-13 bps	1-1.5 bps
€250	1-6 bps	0.5-1 bps
€500	Less than 1bps	Less than 0.5 bps

If the acquirer is able to keep fraud instances within the parameters outlined above, they may apply TRA as a substitute for SCA.

SCA DEADLINES

The SCA standards imposed under the PSD2 were originally set to go into effect in the EU on September 14, 2019. Due to COVID-19 and other extenuating circumstances, though, the deadline for adoption in the EU was pushed back to December 31, 2020. In the United Kingdom, the deadline has been delayed even further (September 2021, as of this writing).

3-D SECURE 2.0

3-D Secure Version 2.0 was mandated in the EU in April 2019. The purpose of this move was to help online businesses streamline the implementation of SCA.

3-D Secure Version 1.0 was not popular with merchants, many of whom believed that increased friction during checkout offset the potential benefits. The most recent version as of this writing, 3-D Secure 2.2, aims to address some of these shortcomings by offering:

- ✓ Greater data sharing to facilitate more accurate decisioning
- ✓ Support for more advanced authentication methods
- ✓ Less disruptive authentication flows

> Roughly 80% of issuers plan to invest in machine-learning and rules-based engines to facilitate SCA processes by the end of 2021.

Ongoing Problems with SCA Adoption

The Indian government enacted a requirement similar to Strong Customer Authentication back in 2014. When that happened, some businesses reported an overnight conversion drop of more than 25% [4]. If we transpose that to the European market, a 25% drop in conversion would have equated to a potential €150 billion economic loss in 2019.

We can expect that some hiccups will be inevitable with any major change to operations in the payments space. Some of these issues will be sorted with time; however, initial reports from the SCA adoption process are not encouraging.

Those operating in the payments space have a lot of work ahead of them to get everyone on board with SCA standards. As Microsoft Director of eCommerce and Payments Dean Jordaan explains, “SCA readiness is more than just EMV 3DS enablement, it is about performance as well.” He suggests that the entire payments ecosystem still “has some ways to go” before we achieve a workable state.

SUCCESS LOW; ABANDONMENT HIGH

In December 2020, Microsoft Director of eCommerce and Payments Dean Jordaan published the company’s SCA Scorecard, outlining their tests with SCA in the European market [5]. The results raised concerns within the payments space:

✓ **Authentication success rates are low**

Microsoft was able to authenticate 76% of browser-based transactions using SCA. For app-based (mobile and gaming console) transactions, that figure dropped to 48%. Their experience suggests that SCA enforcement will introduce substantial friction into the process.

✓ Authentication abandonment remains high

Customers abandoned 14% of browser-based transactions, and 25% of app-based transactions, when asked to verify themselves according to SCA requirements. This suggests customers are still uncomfortable providing the verification requested.

✓ Challenge rates remain high

Challenge rates for browser-based and app-based transactions sit at 72% and 73%, respectively. This suggests issuers have yet to optimize their decisioning process when it comes to SCA authentication.

The scorecard also notes that attempts at authentication stand-in remain high in a variety of nations across the continent. This suggests that customers in a number of markets, and at varying levels of national GDP, are not enrolled in SCA protocols.

CONFUSION ABOUT SCA LIABILITY

Surprisingly, it's not always clear when determining the party liable for incidents in which an exemption is applied to avert SCA requirements.

Liability for transactions that are subject to SCA rests with the issuer or acquirer. An acquirer may accept liability for a transaction as a way to exempt SCA requirements. The acquirer may retain that liability, or pass the liability (or resulting costs) on to the merchant. That said, final say still lies with the issuer, which possesses the power to overrule the acquirer and insist on authentication.

NO IMPACT ON FRIENDLY FRAUD

Data from Fi911® suggests that global chargeback issuances will see a compound annual growth rate (CAGR) of 16.3% annually between 2018 and 2023. The majority of these cases will be instances of friendly fraud (61% in North America and 73% in Europe).

The conditions we outlined above will likely improve with time as all parties get acclimated to SCA protocols. Friendly fraud is different, though; unfortunately, SCA will have little impact on this problem, as pre-transaction authentication can't prevent a post-transactional threat like friendly fraud. With friendly fraud set to represent a greater share of chargebacks over time, this promises to gradually wear away the efficacy of SCA practices.

Leveraging Future Opportunities

One recent study published by Ekata examined payment service providers' attitudes to strong customer authentication as a potential strategic opportunity. In the study, they divided respondents into four distinct categories: leaders, laggards, question marks, and challengers [6].

On one hand, the portion of PSPs described as "Question Marks," meaning that they have an unclear position in regards to whether they regard SCA a strategic opportunity, declined slightly. PSPs in this category declined from 42% to 38% between January 2020 and October. At the same time, the "Leaders"—those who regard PSD2 and SCA as an opportunity to reinforce their leadership position in the industry—declined as well; from 22% to 19%. The number of "Leaders" now matches the number of "Laggards" (those who offer no differentiating options in regard to SCA).

TRA IS ESSENTIAL

Financial institutions who leverage SCA effectively can enjoy a competitive advantage. One of the keys to this moving forward should be Transaction Risk Analysis.

As discussed earlier, TRA can be an efficient and effective method of screening for fraud without increasing the risk of introducing unnecessary friction into the transaction process. Thus, adherence to standards for TRA fraud metrics should be seen as a value-add. At the same time, a lack of adherence to TRA fraud metrics could motivate merchants to switch their traffic to an alternative service provider.

Transaction Risk Analysis (TRA) presents the opportunity to achieve higher exemptions and also reduce fraud. This process could then become a competitive advantage for financial institutions moving forward in 2021 and beyond.

MORE EMPHASIS ON CONSUMER EDUCATION

As Juniper Research Lead Analyst Nick Maynard notes, SCA compliance alone will "not be enough to guarantee effective fraud prevention in many cases [7]." Instead, he suggests that businesses operating in payments and finance should "focus on creating solutions above and beyond the basic regulatory requirements."

We noted earlier that customers abandoned 14% of browser-based transactions, and 25% of app-based transactions, when asked to verify themselves according to SCA requirements. As these figures suggests, a major part of the problem is a lack of consumer awareness of SCA protocols.

A recent report by Stripe found that 73% of consumers are not aware of the new authentication requirements. Furthermore, 74% of Gen-Z shoppers have abandoned an online purchase at checkout due to a bad experience [8]. These two facts help illuminate the challenge experienced by merchants, and the financial institutions who support them, as a result of SCA requirements. At the same time, they make it clear that educating consumers about strong customer authentication could be transformative.

How Financial Institutions Can Help

Data published by Mastercard in December 2018 revealed that up to 75% of European merchants remain unaware of SCA and how they should prepare for it. More than half of those surveyed said they would either not be ready before the deadline, or "have zero plans to support" SCA standards [9].

Although conditions have changed in the last two years, this figure still does not bode well for the state of merchant SCA adoption. Acquirers will need to step up and play a pivotal role in getting merchants on board with SCA.

These are the top five functionalities that PSPs say they will provide to merchants to help with adjustment to PSD2 and SCA:

- ✓ 3-D Secure (+90% will offer by October 2021)
- ✓ Rule-Based Fraud Screening (+80%)
- ✓ Transaction Risk Assessment (TRA) (+80%)
- ✓ Exemption Management (+80%)
- ✓ Delegation of Exemption (+70%)

There are a number of other things that financial institutions can do to help with the move to strong customer authentication standards, too. We recommend that institutions:

EDUCATE MERCHANTS ON NECESSARY ACTIONS

Acquirers can help merchants navigate the minimum actions needed to take to ensure SCA application, and to prevent unnecessary declines.

EXPLAIN THE OUTLIERS

Transactions outside the purview of SCA, such as merchant-initiated transactions, require a degree of nuance in understanding. Merchants must know how to handle these scenarios to guard against unnecessary declines.

HELP WITH RESCREENING

Rescreening orders can help authenticate buyers who would otherwise have been rejected. Sophisticated rescreening efforts will help merchants recover valid sales.

EMPHASIZE THE CUSTOMER EXPERIENCE

This should come as no surprise, but it is important to underscore the value of providing positive customer experiences and to streamline interactions with buyers.

DISTINGUISH “POSITIVE” AND “NEGATIVE” FRICTION POINTS

Some level of friction is unavoidable with SCA. The entire idea is to create a measure of friction to deter fraudsters. So, rather than resisting friction outright, financial institutions should try to redirect it in a more positive direction.

There’s a difference between “positive” and “negative” friction. The latter slows down processes for no reason, driving a wedge between merchants and buyers. The former creates a reasonable degree of friction that is hardly noticeable from the buyer’s perspective, but which can be very effective at stopping fraud.

Examples of positive friction include:

- ✓ Verifying CVV at checkout
- ✓ Asking buyers to verify their order before finalizing
- ✓ Making account creation optional
- ✓ Requiring complex and unique passwords for all new accounts
- ✓ Offering 3-D Secure 2.0 for users who opt-in to the service
- ✓ Employing backend fraud tools (geolocation, IP verification, fraud scoring, etc.)
- ✓ Offering mobile payments with two-factor authentication

ABOUT Fi911

Fi911 supports financial institutions with innovative back-office management technologies created specifically for the banking and payments industries. Fi911's proprietary DisputeLab™ helps make resolving chargeback disputes faster and more efficient by optimizing each step in the dispute cycle. The company's unified platform also provides threat detection, reconciliation, and risk management tools, as well as the ability to generate commissions and ISO pay-outs directly through the system. Established by the dispute experts at Chargebacks911®, Fi911 offers global reach and expertise, as well as customized training and support from recognized industry leaders. For more information, visit www.Fi911.com.

Sources

[1] https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46776.pdf

[2] https://thepaypers.com/expert-opinion/where-is-fraud-heading-after-psd2s-strong-customer-authentication—1240339

[3] https://www.statista.com/statistics/239247/global-online-shopping-order-values-by-device/

[4] https://www.pymnts.com/news/regulation/2019/strong-customer-authentication-compliance-stripe/

[5] https://www.linkedin.com/pulse/microsoft-sca-testing-results-dean-jordaan/

[6] https://www.finextra.com/researcharticle/172/unlocking-the-potential-of-psd2-and-sca-the-five-markers-for-success

[7] https://thepaypers.com/expert-opinion/where-is-fraud-heading-after-psd2s-strong-customer-authentication—1240339

[8] https://www.finextra.com/the-long-read/68/beyond-invisible-solutions-banks-should-be-preventing-fraud-not-playing-catch-up

[9] https://newsroom.mastercard.com/eu/press-releases/majority-of-european-retailers-unaware-of-new-payment-standards-coming-into-force-in-september-2019/

Fi911™
fintech solutions

18167 US Highway 19 N. Clearwater, FL 33764
877.634.9808 | info@chargebacks911.com