Implementing Strong Customer Authentication (SCA) Exemptions

ACI Worldwide
Real-Time Payments

Contents

- Alignment

- Five steps to implement SCA exemptions ahead of the PSD2 deadline

   1. Balance customer experience and compliance

   2. Implement a strategy and solution

   3. Address ambiguity with scoring

   4. Understand liability to mitigate risk

   5. Integrate EMV 3DS

- Key takeaways

Implementing Strong Customer Authentications
(SCA) Exemptions
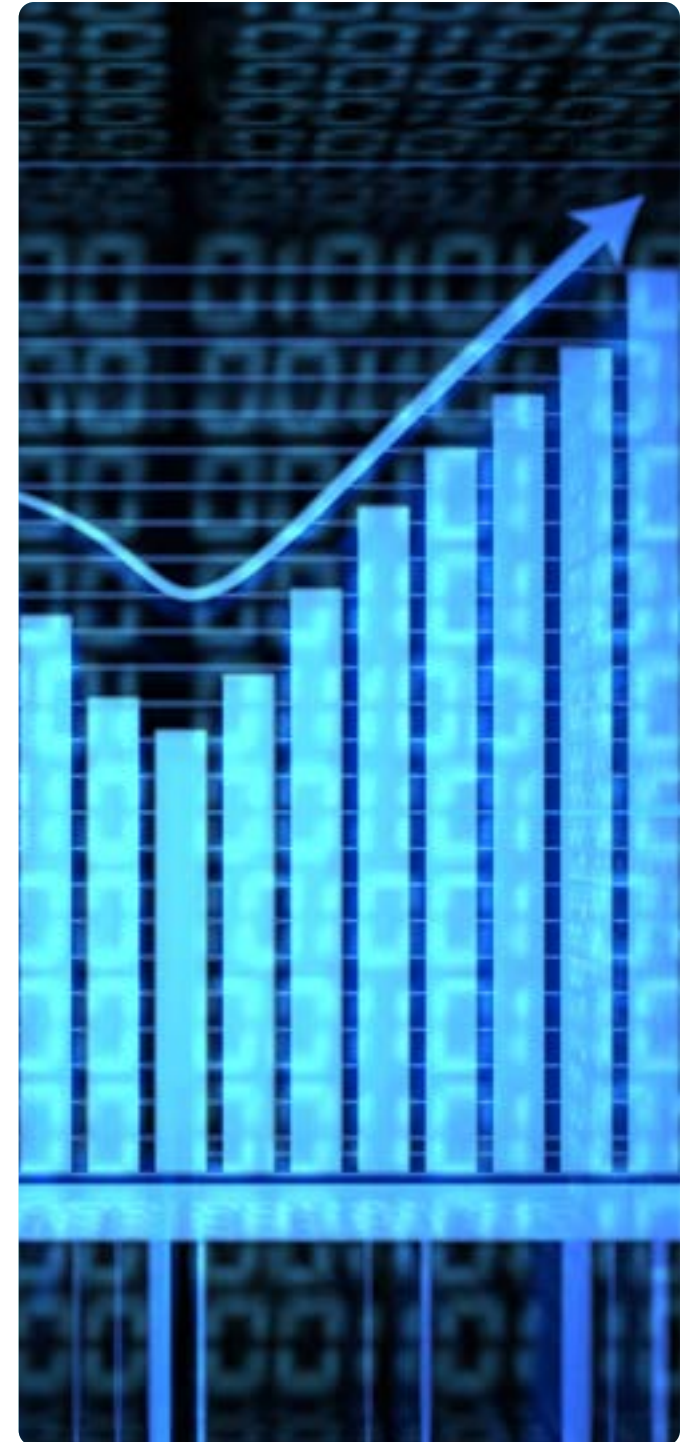
Topics
Covered in eBook

PSD2[1] RTS SCA and exemptions
Focus on card payments

European Banking Association (EBA) insight
The impact of the EBA's opinion document on SCA strategies

Deadlines
Under review and are set to be extended, similarly to the U.K.

[1]Payment Services Directive 2

Intended Audience
within the payments value chain

This resource is primarily intended for issuing and acquiring banks and payment service providers (PSPs) but is relevant for eCommerce merchants.

Terminology can differ depending upon region.

PSD2 RTS SCA and exemptions apply to both card and non-card payments.

Please contact
Jay.Floyd@aciworldwide.com if there are any questions around strong customer authentication (SCA)/exemptions for non-card (digital) payments.

Protect the Customer Experience and Gain Competitive Advantage

Five steps to implement SCA exemptions ahead of the PSD2 deadline

Many consumers can feel frustrated with current authentication approaches. For card payments, this is typically done through 3DS (3D Secure, versions 1 and 2) via specific characters in a static password or one-time password (OTP) via SMS or text message.

Applying SCA for all transactions over €30 may prove unacceptable and result in **increased abandon rates**, or in **consumers choosing to shop elsewhere** or **with a different card**, ultimately risking loss of market share.
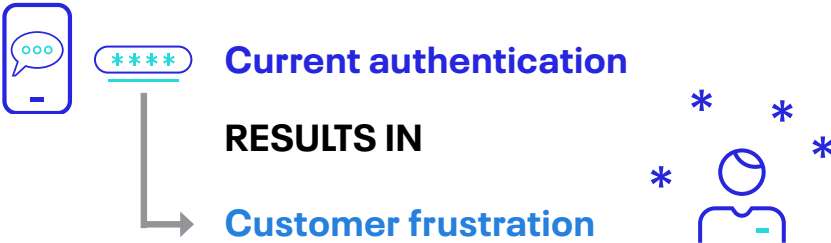
Balance Customer Experience and Compliance
Will PSD2 SCA impact customer experience?

1

A compliant strategy is based in **adopting inherence (biometrics)** or, as some financial institutions are considering, **implementing acceptable possession and knowledge elements**, e.g., OTP via SMS (to meet the possession requirement) and a password/personal identification number (PIN) (to meet the knowledge requirement).

Current authentication

RESULTS IN

Customer frustration

Authentication methods
incorrectly applied

Inherence
(biometrics)

OTP via SMS

Password/PIN

Exemptions are key to balancing the customer experience (CX). Compliance and and fraud prevention should always be included as part of the overall regulatory technical standard (RTS) SCA implementation strategy.
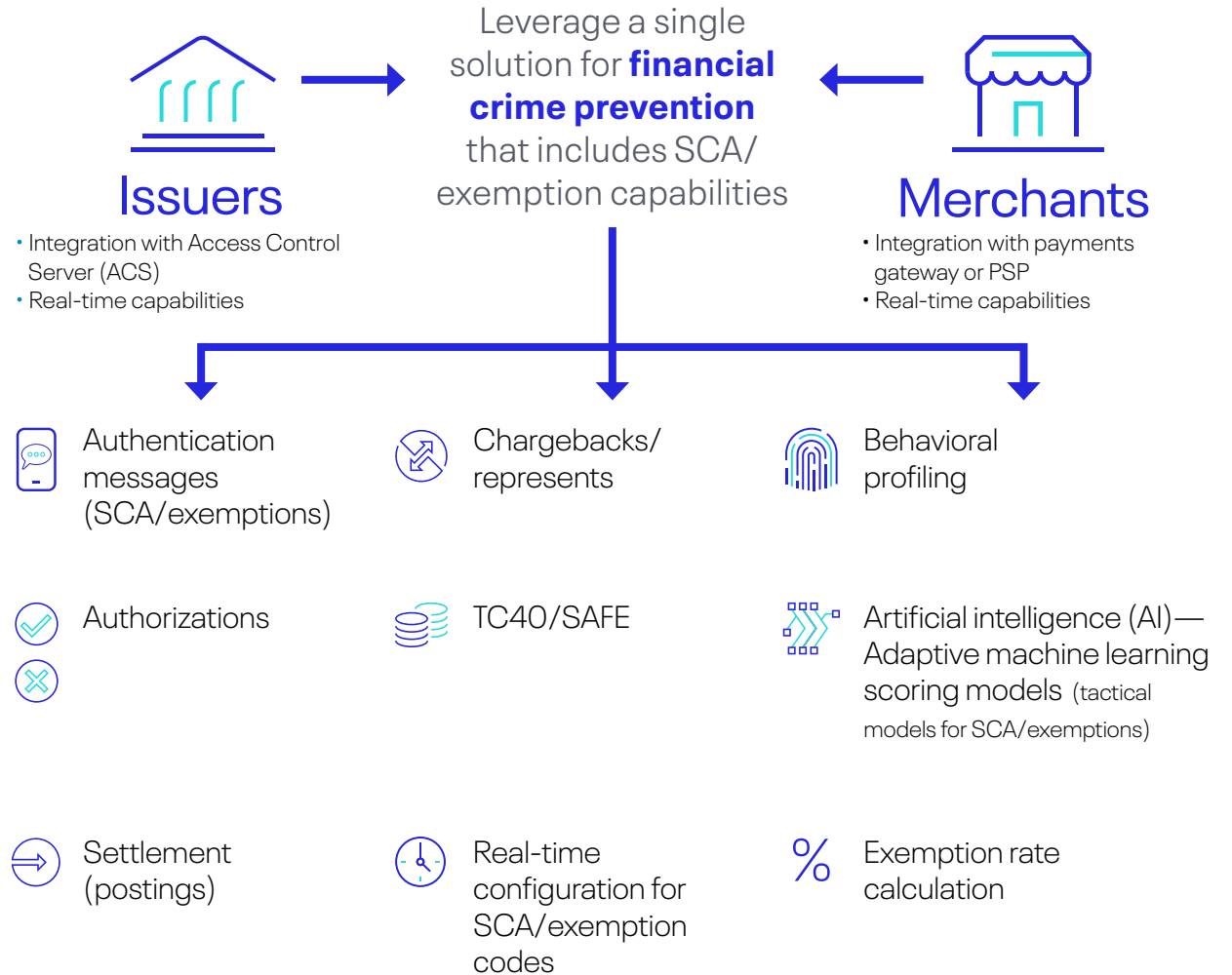
Implement a Strategy and Solution
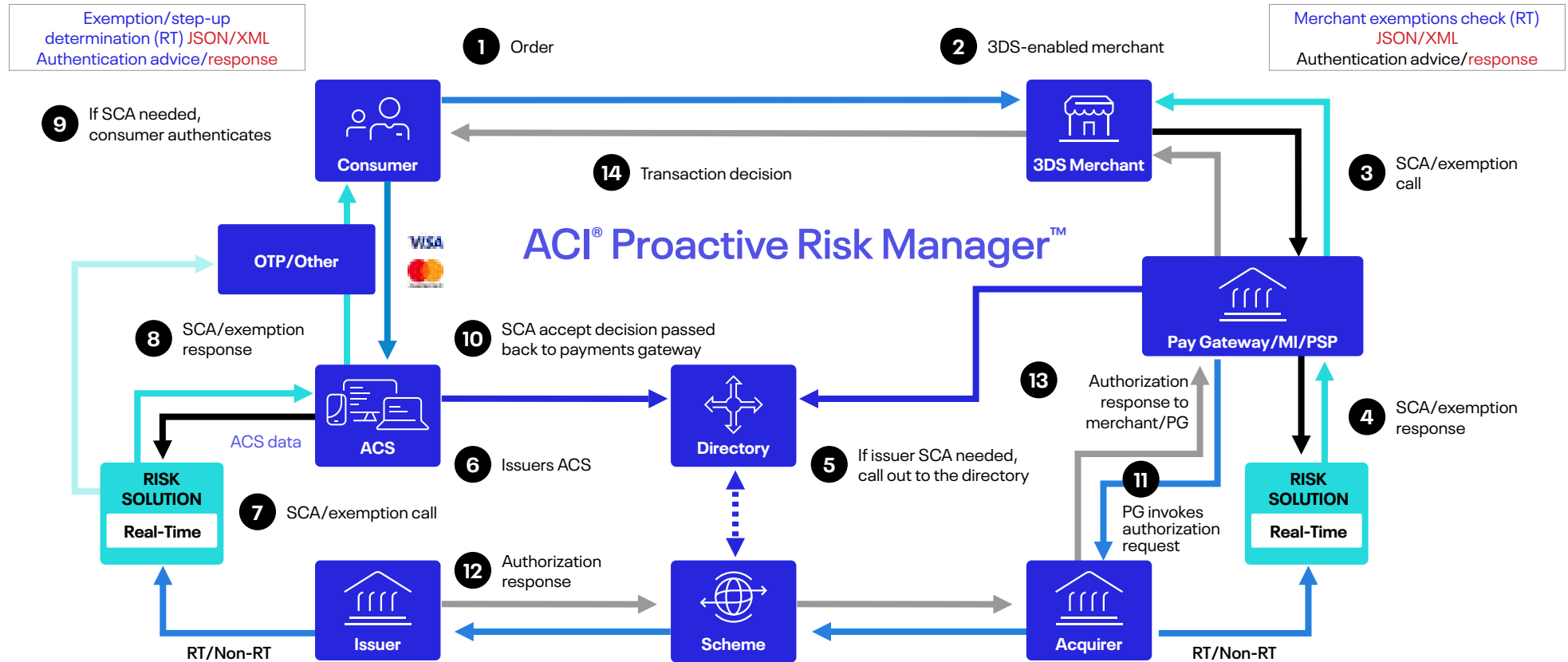## How do I deploy an exemptions strategy?

Technology As An Enabler

The right technology can enable fraud prevention and exemption strategies. Everything must be done in real time (RT). It's critical to lead with a strategy that prioritizes maintaining and improving the CX, to help both issuers and merchants reduce customer attrition and grow market share.

Issuers
- Integration with Access Control Server (ACS)
- Real-time capabilities

Leverage a single solution for **financial crime prevention** that includes SCA/exemption capabilities

Merchants
- Integration with payments gateway or PSP
- Real-time capabilities

- Authentication messages (SCA/exemptions)
- Chargebacks/ represents
- Behavioral profiling

- Authorizations
- TC40/SAFE
- Artificial intelligence (AI)— Adaptive machine learning scoring models (tactical models for SCA/exemptions)

- Settlement (postings)
- Real-time configuration for SCA/exemption codes
- Exemption rate calculation

PSD2 RTS-SCA and Exemptions—EMV 3DS Scenario
Both legs in (issuer and merchant both in the EU)

1 Order

2 3DS-enabled merchant

Exemption/step-up determination (RT) JSON/XML Authentication advice/response

Merchant exemptions check (RT) JSON/XML Authentication advice/response

9 If SCA needed, consumer authenticates

Consumer

14 Transaction decision

3DS Merchant

OTP/Other

VISA

ACI® Proactive Risk Manager™

3 SCA/exemption call

Pay Gateway/MI/PSP

8 SCA/exemption response

10 SCA accept decision passed back to payments gateway

13 Authorization response to merchant/PG

4 SCA/exemption response

ACS data

ACS

6 Issuers ACS

Directory

5 If issuer SCA needed, call out to the directory

11 PG invokes authorization request

RISK SOLUTION Real-Time

RISK SOLUTION Real-Time

7 SCA/exemption call

12 Authorization response

Issuer

Scheme

Acquirer

RT/Non-RT

RT/Non-RT

The above diagram illustrates the typical flow for EMV 3DS authentication and subsequent card authorization. However, the key difference here is how the payments gateway/merchant integrator/PSP can call out to ACI Fraud Management for an SCA/exemptions decision in real time. Likewise, issuers' ACS (Access Control Server) can also call out to ACI Fraud Management for an SCA/exemptions decision in real time. Combining this authentication data with the card payment authentication provides enhanced data intelligence for sophisticated fraud prevention strategies.

3 Address Ambiguity with Scoring
Do I need to implement new scoring for Article 18?

> **"**
> The assessment made by a PSP shall combine all those risk-based factors into a risk score for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication."
>
> **EBA, Single Rulebook**

AN EXEMPTIONS STRATEGY CAN INCLUDE AN OPTIONAL TRANSACTION RISK ANALYSIS (TRA) AS DEFINED UNDER ARTICLE 18 AND DERIVE A SCORE THAT CAN BE LEVERAGED TO EITHER APPLY EXEMPTIONS OR TRIGGER SCA.

To achieve this, organizations should implement a **financial crime prevention solution that allows robust TRA** as defined under Article 18 and more.

Can your fraud prevention technology do the all of this?

- Create and maintain your own behavioral profiles
- Data retention and historical interactions
- Digest information from multiple data sources for enhanced intelligence
- Create and maintain your own tactical AI adaptive machine learning scoring models

4 Understand Liability to Mitigate Risk
Which party is liable for fraud losses based on the authentication flow?

Use Case	Merchant		Liability
Standard-3DS	→	Initiates 3DS	Issuer
Merchant not 3DS-enabled	→	Cannot apply 3DS	Acquirer/Merchant
Merchant/PSP/acquirer exemption	→	Initiates 3DS flow with exemption	Issuer if they override and conduct SCA
Merchant/PSP/acquirer SCA	→	Authenticates consumer with SCA	Issuer if they override and conduct SCA

If a merchant/PSP/acquirer/issuer is not compliant by the deadline, potential consequences are:

Loss of license

Potential fines

Non-compliant party

5 Integrate EMV 3DS
What are the alternatives to EMV 3DS?

Online Purchases

EMV 3DS appears to be the **go-to strategy** for organizations processing online purchases.

Merchant Mobile Apps

EMV 3DS does not appear to be the go-to strategy for organizations when processing mobile app purchases. **SCA must still be applied where needed**, but can be in the form of other combinations of knowledge and possession vectors.

Biometrics

Wallets

PINS

Key Takeaways
What **you need to know** about PSD2 SCA exemptions

Customer Experience + Compliance

If you **do not offer exemptions**, companies run the risk of **impacting CX** and **reducing revenue**.

Managing exemptions

Managing exemptions is critical and can be rapidly and easily adopted with the right technologies and partners. **Without a strong SCA exemptions solution, you cannot deliver on CX**.

The Recipe for Success
Three key ingredients

1

Identify, **accept** and **embrace** the need for exemptions

2

Adopt the **best approach and strategy** and engage with the right technology partner, like ACI, to assist

3

Implement before deadline to ensure compliance

How to Solve for SCA Exemptions

WITH THE RIGHT TECHNOLOGY IN PLACE TO MAKE REAL-TIME DECISIONS AND WITH SUPPORT FROM A KNOWLEDGEABLE PARTNER, IMPLEMENTING EXEMPTIONS AHEAD OF THE REGULATORY DEADLINE CAN BE EASY.

Many see exemptions as "just another challenge to overcome," but it is worth thinking strategically now to **avoid creating future complexity** as a result of a poor tactical decision. Reverting the impact of a poor decision now will be painful in the future.

The ACI Fraud Management solution has a proven track record of excellence in managing customer attrition related to fraud prevention. This experience now benefits the acquirers as they look to achieve compliance and manage customer experience in parallel, to minimize the impact of SCA and capitalize on the opportunity of exemptions. This creates an accelerated path to market leadership.

ACI Worldwide
Real-Time Payments

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com

@ACI_Worldwide

contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393