SOLUTION BRIEF

Meeting PSD2 SCA & Open Banking Requirements with RSA® Fraud & Risk Intelligence Suite

As part of the European Union (EU) revised Payment Services Directive (PSD2), the enforcement of new authentication requirements went into effect September 14, 2019, and will significantly impact financial institutions, payment providers, financial technology (fintech) companies and consumers. The scope of PSD2 aims to streamline electronic payments more effectively across European markets through these main objectives:

- Enhanced payment safety and security
- Consumer protection and reduced fraud
- Improved ecosystem with more innovation and new competition

The European Banking Authority (EBA) further announced on October 16, 2019, that new Strong Customer Authentication (SCA) for e-commerce card-based transactions should be fully enforced by December 31, 2020.[1] Understanding the complexity and challenges regarding online payments across EEA countries, the EBA recommends a consistent approach focused on monitoring SCA implementation plans instead of pursuing immediate enforcement against payment providers that are not compliant with the requirements. Noncompliance could carry business risk with losing transaction volume, imposed fines or even rescinded payment licenses. However, the EBA will provide limited additional time to meet SCA requirements, but only on special exceptions, to allow organizations to find the right solution and implement it the right way.

Strong customer authentication

The one crucial PSD2 mandate is enforcing Strong Customer Authentication (SCA). This is a form of authentication that uses two or more of the following elements: knowledge (e.g., password), possession (e.g., mobile device) and inherence (e.g., fingerprint). Each of these elements should be independent, the compromise of one element should not compromise another element, and the integrity of the authentication data should be protected. The purpose of SCA is to further protect the consumer as evolving technology and demand for convenience reveal new risk vectors. Organizations will have to find balance between security and "user-friendly" customer experience while also meeting regulation requirements. Effectively managing SCA compliance will impose a significant burden on organizations for each transaction performed:

- Additional security requirements add friction to the authentication process.
- Transaction abandonment rates may increase.
- More call center resources may be required to handle the potential increase in the number of failed authentications and lockouts.

Organizations that demonstrate low fraud rate thresholds can lessen the negative impact by leveraging SCA exemptions for transaction risk analysis, or in other words, risk-based authentication. By taking a layered, risk-based approach to authentication, organizations can better identify fraud, validate transactions and deliver a seamless user experience across digital channels. Increasing visibility into online activities helps distinguish between fraudsters and cybercriminals to genuine users, which successfully helps mitigate financial losses stemming from fraud losses, brand damage, transaction abandonment, operational expenses and negative consumer experience.

Four key areas of focus for addressing SCA

PSD2 defines very specific SCA requirements, and organizations seeking to implement the regulation requirements are required to focus on four key areas: Dynamic Linking, Leveraging Fixed Exemptions, Transaction Monitoring and Transaction Risk Analysis.

Dynamic linking

This requirement outlines security measures for when transactions are initiated and carried out between payer and payee. Dynamic Linking helps organizations reduce fraud rates by preventing man-in-the-middle attacks that interrupt customer transactions by modifying payee information and/or transaction amount to execute fraudulent payments. It is essential that organizations protect transaction data between both parties and demonstrate they are meeting SCA requirements, ensuring the following obligations:

- The payer is made aware of the amount of the payment transaction and of the payee.
- The authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.
- The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer.
- Any change to the amount or the payee shall result in the invalidation of the authentication code generated.
- When the authentication fails, the elements for knowledge, possession or inherence cannot be identified.

Organizations can validate high-risk transactions employing the transaction signing functionality in RSA Adaptive Authentication, which verifies the authenticity and accuracy of transaction details. This feature provides integrity assurance, cryptographic signature and authenticity for payment transactions to combat fraud from advanced financial malware attacks. Transaction signing can optionally integrate with biometrics, such as fingerprint or Face ID, as a stronger means of authentication layered on top of the payment transaction signature. RSA Adaptive Authentication supports a range of modern authentication methods including biometrics, out-of-band authentication with SMS or push OTP sent to the consumer's mobile device, and more.

Leveraging fixed exemptions

Consumers demand convenience, security and transparency from financial institutions despite what regulatory requirements mandate. Authentication methods must be well-matched with the level of risk involved. However, balancing security with user convenience is no simple feat. Financial institutions and payment providers can ill afford to add friction to consumers' payment process and letting it impact the level of customer service they deliver.

The Regulatory Technical Standards (RTS) outline fixed exemptions that would allow certain types of transactions to occur without adhering to the SCA requirement for two-factor authentication. For example: Low-value transactions, less than five transactions of €30 or less, will not require SCA to be applied. In addition, merchants and businesses that have repeat customers and specific transaction types with variable amounts will have the opportunity to avoid multiple authentication requests. Financial institutions can leverage these exemptions to maintain a "user-friendly" experience that minimizes friction for online banking, payments and e-commerce transactions.

Through the use of a comprehensive rules framework, the Policy Management Application featured in RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce translates risk policies into decisions and actions. With fine-grained policy capabilities, organizations can set rules based on SCA exemptions to reflect business objectives such as identifying fraud prevention targets, improving user experiences and controlling operational costs associated with case analysis.

Transaction monitoring

Financial institutions and payment providers are required to have transaction monitoring methods in place that detect unauthorized or fraudulent transactions. They will also need to include ongoing reporting of fraud rates to evaluate compliance to use the exemption for SCA. Maintaining low fraud rates means less fraud losses while maintaining frictionless interaction for genuine users and lower operating costs associated with reviewing transactions. With that said, the fewer genuine transactions are challenged in the process of blocking fraudulent ones, the better for everyone.

The RSA Risk Engine is a central component of RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce. The RSA Risk Engine drives outstanding fraud detection performance through a powerful combination of diverse data inputs and machine-learning methods for continual improvement. Using a variety of sources of information, the RSA Risk Engine assigns a unique risk score to every digital transaction. The risk score and the risk policy set by an organization together determine whether a user is challenged with step-up authentication.

The RSA Risk Engine takes as many factors as possible into consideration: payment activity, nonpayment activity, geolocation, cross-channel information, RSA case management feedback, device profile, mobile activity, third-party risk indicators, IP information and RSA eFraudNetwork™ when assigning the most accurate risk score to every user's digital activity.

Transaction risk analysis

Beyond fixed exemptions, Transaction Risk Analysis (TRA) is a method used for identifying fraud by analyzing many different elements of a transaction including both payer and payee involved in the transaction. Payment providers can use TRA to secure online payments, but it will be essential to keep their fraud rates low enough. The EBA has specified transaction value thresholds up to €500 based on fraud rates where this exemption can apply. For example, if a bank achieves a 3 basis-point fraud rate, the bank qualifies for a transaction risk analysis exemption for SCA up to €250. This means that financial institutions can leverage TRA only if they meet low fraud rates. If they do not, then SCA is required, which adds friction to the consumer experience.

RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce rely on the RSA Risk Engine to assign an accurate risk score to every transaction and as such can help organizations meet the required fraud rates so they can leverage the exemption. With RSA Adaptive Authentication and RSA Adaptive Authentication for eCommerce, organizations can reach over 95 percent fraud detection rates, with an intervention rate of only 5 percent.[1]

What does this mean for merchants?

Although merchants are not directly subject to PSD2, they should be concerned that transactions could be declined by financial institutions. They need transactions to either qualify for an exemption or validate that SCA successfully occurred. If neither of these requirements is met, then approving the transaction would mean violating the regulation. Regardless of avoiding being noncompliant with the regulation, financial institutions should feel comfortable approving transactions, protecting against fraud and balancing the business impact.

By merchants adopting EMV 3-D Secure, financial institutions can enforce strong customer authentication and meet the PSD2 requirements. Embracing the new EMV 3-D Secure protocol can help merchants avoid increases in transaction decline rates and help financial institutions meet regulation requirements.

RSA Adaptive Authentication for eCommerce brings card issuers and payment processors the high fraud detection, low intervention advantages of the RSA Risk Engine for e-commerce transactions. It supports the 3DS 2.1 and 2.2 protocols, reliably authenticating e-commerce transactions without cumbersome customer processes. RSA Adaptive Authentication for eCommerce:

- Promotes secure transactions with a 2:1 ratio of genuine to fraudulent transactions
- Supports a secure, frictionless digital shopping experience for consumers
- Saves an average of $2 million in fraud losses per customer, per month
- Minimizes fraud losses to just $3.55 for every $10,000 earned in legitimate transactions[2]

Open banking

Aimed toward increasing competition and innovation in European markets, PSD2 includes a significant transformation to help the financial industry streamline an evolving landscape and meet consumer expectations for instant transfers, seamless experiences and accessibility from anywhere. This change requires financial institutions to open up bank data using application programming interfaces (APIs) that afford consumers secure access to their bank accounts and information through third-party providers (TPPs) with the consent of the account owner.

Open APIs enable banks and fintechs the capability to integrate and work together, creating new ways that provide convenience for consumers, drive adoption and further the investment in modernization.

However, capitalizing on delivering convenience for consumers elevates the threat that fraudsters and cybercriminals can exploit the opportunity, and the risk must be mitigated and managed. RSA Adaptive Authentication enables financial institutions to assess the risk associated with transactions and online activities originated from APIs.

Supporting risk-based authentication to address SCA

Investing in effective fraud detection and prevention tools is critical to financial institutions seeking to remain competitive and leverage regulation exemptions to find the right balance between compliance requirements and consumer convenience.

RSA delivers risk-based authentication and a variety of step-up authentication methods that help customers determine how they can address the requirements of SCA while maintaining a user-friendly experience that minimizes friction for online banking, payments and e-commerce transactions.

RSA Adaptive Authentication

Is an advanced, omnichannel fraud detection hub that provides risk-based, multi-factor authentication for organizations seeking to protect their consumers from fraud across digital channels. Powered by the RSA Risk Engine, RSA Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators. Using powerful machine learning and fine-grained policy controls, the RSA Adaptive Authentication anti-fraud hub only requires additional assurance, such as out-of-band authentication and transaction signing, for scenarios that are elevated risk and/or violate rules established by an organization. This methodology provides transparent authentication for most of the users, ensuring a frictionless end-user experience and high fraud detection rates.

RSA Adaptive Authentication for eCommerce

Is RSA's 3-D Secure solution for credit/debit card issuers and issuing processors. Utilizing the 3-D Secure protocol and infrastructure, RSA Adaptive Authentication for eCommerce enables credit/debit card issuers to provide a consistent, secure online shopping experience for cardholders while mitigating the risk of chargeback losses. Powered by the RSA Risk Engine, RSA Adaptive Authentication for eCommerce provides a frictionless shopping experience by silently authenticating genuine cardholders while challenging only the minority of transactions that are high risk or cannot take advantage of any regulatory exemptions. Its ability to accurately challenge and eliminate fraud while providing genuine cardholders with a frictionless shopping experience is unmatched in the industry.

Conclusion

Financial institutions, payment providers and fintech companies are actively assessing the impact of PSD2 SCA requirements on their business, transaction processes and security operations. With a looming deadline of December 31, 2020,[4] for card transactions, and the September 14, 2019, deadline already surpassed for digital banking channels, organizations need help deploying strong customer authentication methods compiled with fraud prevention and monitoring tools to avoid fines, fraud losses or a decline in transaction volume due to failed authentication. Balancing the regulation requirements with customer experience, operational costs, fraud losses and revenues is key to being successful and innovative in a highly competitive market.

About RSA Fraud & Risk Intelligence Suite

RSA® Fraud & Risk Intelligence Suite enables organizations to manage risk across consumer-facing digital channels, allowing them to maximize revenues and minimize fraud losses. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

[1] Some countries declared exceptions; for example, the UK declared September 14, 2021, for card-based transactions, and France will offer one three-month waiver on a case-by-case basis.

[2] Fraud detection rates are not guaranteed; it depends on customer implementation, overall fraud rates and patterns.

[3] RSA data on average fraud losses 15H2 – 17H1

[4] Some countries declared exceptions; for example, the UK declared September 14, 2021, for card-based transactions, and France will offer one three-month waiver on a case-by-case basis.