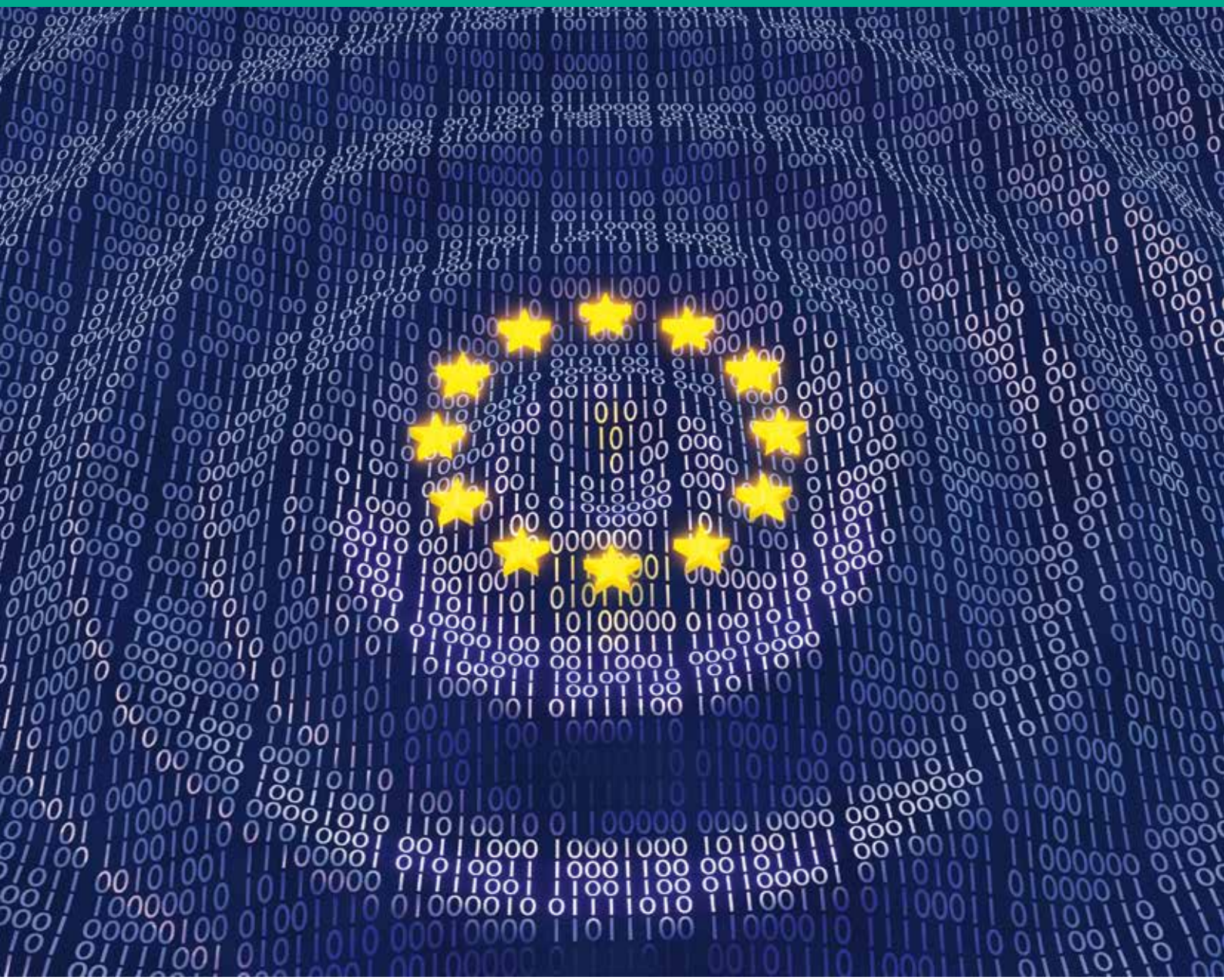

PSD2, Open Banking and APIS:

Can You Navigate the Maze of Fraud & Security Implications?

kfp.kaspersky.com
#truecybersecurity

So it's been a year since the second Payment Services Directive (PSD2) came into force... With all that talk of the demise of traditional banks and how digital challengers will change the face of banking and financial services forever, where are we now?

Well, it's been a slow start. Undeniably, January 13, 2018 was a momentous date, with everyone getting busy trying to understand how and when strong customer authentication applies (is it good? Is it bad? Who benefits?), and pondering whether giving third parties access to bank accounts via APIs or other suitable interfaces is something that would break (or benefit) the well-established ecosystem. And there was a lot of confusion, which was exacerbated with the coming into force of the General Data Protection Regulation (GDPR) on May 25, 2018, and the increased stringency of Anti-Money Laundering regulations worldwide. Last year certainly was a challenge for all businesses in all industries, but particularly in financial services. It was nevertheless a good thing: new services taking advantage of Open Banking came on the market, a lot of the confusion got ironed out, some digital challengers did very well out of it, applications for banking licenses became very popular (certainly in Europe), and all sorts of organizations applied to be registered as third-party providers in this suddenly more open payments ecosystem (at least in the UK, if the FCA Register[1] is anything to go by...).

Unsurprisingly, the banks are still here and thriving, and will still be here for many years to come. But what happened in 2018 is an uncanny and pervasive sea change in corporate culture and strategies. This is because over the last few years, the new crop of digital challengers have realized that putting the customer at the center of their vision will win them a lot of good will, and they used technology to generate that good will, unburdened from legacy infrastructure. This didn't happen suddenly. As an example, well-established companies such as Intuit, Trustly, Sofort, Yodlee and Mint had for years relied on what is commonly referred to as 'Screen Scraping'[2]. This doesn't come without risk: as cybercrime continues to evolve at the pace of technology, fraud and identity theft have become an ever-present modern day challenge. This is why the PSD2 RTS set out, controversially (as it would arguably destroy some business models) to ban screen scraping altogether.

In our opinion, this is totally understandable from a security standpoint: with the direct access model, the bank account holder has to share their banking credentials with a third party so that information from the bank account information can be obtained (i.e. 'screen-scraped') so as to provide the service (e.g. a tax return). Understandably, the banks are unhappy with this model because they have no way of knowing whether a customer is accessing their account directly, or through a third party, as the same set of credentials are being used by both.

Before PSD2, these third parties were unregulated. PSD2 brings them under the regulatory umbrella as Third Party Providers (TPPs) and classifies them as Account Information Service Providers (AISPs), such as Intuit, and Payment Initiation Service Providers (PISPs), such as Sofort.

After the announced ban of Screen Scraping by the European Banking Authority, and after industry consultation, a delay was agreed to give time to all parties to develop the new access mechanisms (post-January 13, 2018, when the PSD2 came into force). This is why the requirements of the "Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) and Common and Secure Open Standards of Communication"[3] only come into force in September 2019. However, on March 14, 2019, all account providers (i.e. ASPSPs, aka the banks) with payment accounts accessible online must meet the requirements to make available both technical specifications regarding their access interfaces, and testing facilities for TPPs, and on June 14, 2019, those seeking exemption from the requirements for a contingency mechanism (in case the dedicated access mechanism fails) should aim to submit their application for exemption. With this first piece of the RTS, PSD2 clearly aims to improve the security of the ecosystem with differentiated authentication of the various parties when accessing payment accounts.

The second part of the RTS relates to Strong Customer Authentication (SCA). As we have examined the reasons why a ban on screen scraping was put in place, we can now turn our attention to the ways authentication must be performed. There has been a lot of industry debate on the pros and cons of two or more factors of authentication, but we must not lose sight that the PSD2 aims to preserve the integrity of the payment ecosystem. And therefore all participants in the value chain must ascertain that those accessing payment accounts (for payment or information purposes) are indeed genuine. This is particularly challenging with the rise in cybercrime and the abundance of stolen credentials available on the black markets due to the large data breaches of recent years, invariably leading to Identity Theft.

To address this challenge, the PSD2 mandates SCA for a wide range of online accounts and ecommerce payment transactions and for carrying out any action via a remote channel which may give rise to a risk of payment fraud or other abuse (e.g. initial registration of a card in a wallet).

SCA is based on the use of two or more factors categorized as:

- knowledge (something only the user knows)
- possession (something only the user possesses) and
- inherence (something the user is)

These factors must be non-reusable, non-replicable (except for inherence) and kept securely. This is to ensure that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.

In addition, for remote transactions (e.g. online payments when a user is initiating a funds transfer through their banking app or a card-based payment on a merchant's website), where the risk is higher, the authentication code generated must be specific to the amount of the payment transaction and the payee. This is known as 'dynamic linking'.

Admittedly, the PSD2, whilst intending to increase security and fraud prevention, also aims to be pragmatic and doesn't set out to introduce any unnecessary friction, and therefore, there are a number of exemptions to SCA:

SCA Exemption	RTS	Applicability
Access to payment information	Article 10	Applies when account holder checks the account balance or payment transactions executed in the last 90 days.
Contactless payments	Article 11	Applies to low value contactless transactions up to €50 with a maximum of €150 cumulative spend or 5 consecutive transactions.
Unattended terminals for transit and parking	Article 12	Applies to contact and contactless transactions for paying a transport fare or a parking fee at unattended payment terminals, regardless of amount.
White list of trusted beneficiaries	Article 13	Applies where the payee is on a list of 'trusted beneficiaries' managed through the payer's PSP or ASPSP.
Recurring transactions	Article 14	Applies if the transaction is one of a series of transactions made with the same payee and the same amount, subject to applying SCA when the payer creates, amends or initiates a series of transactions.
Credit transfers to self	Article 15	Applies when the payer sends a credit transfer to themselves and both sending and receiving accounts are held by the same ASPSP.
Low-value remote transactions	Article 16	Applies to remote transactions up to €30, with a maximum of €100 cumulative spend or 5 consecutive transactions since SCA was last applied.
Commercial transactions	Article 17	Applies to payers who are not consumers where competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those achievable with SCA.
Transaction Risk Analysis (TRA)	Article 18	Only applies to remote payments and depends on fraud levels.

From the table above, it becomes evident that, as with any sensible security risk posture, the intent of the regulation is to promote the deployment of a layered security approach, based on the risk presented by a particular activity. In simple terms, risk-scoring can take advantage of data that is available during or before authentication. For example, device information, geo or IP location, behavioral biometrics, and analysis and scoring using machine learning or artificial intelligence can provide valuable insights when determining the risk associated with a transaction.

1 **https://register.fca.org.uk/shpo_searchresultspage?preDefined=AIPISP&TOKEN=3wq1nht7eg7tr**
2 Also known as "Direct Access"
3 **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389**

More specifically, if PSPs want to use the Transaction Risk Analysis (TRA) exemption, they must be able to identify that the transaction poses a low risk. In order to do so, PSPs must ensure that:

- The fraud rate for that type of transaction does not exceed the reference fraud rates specified in the RTS and
- The transaction amount doesn't exceed the Exemption Threshold Values (ETVs), and
- PSPs must perform real-time risk monitoring and analysis and be satisfied that:
  - The payer doesn't exhibit any abnormal spending or behavioral pattern, and
  - There is nothing unusual about the payer's device or software access, and
  - There is no malware infection in any session of the authentication procedure, and
  - There is no known fraud scenario in the provision of the payment service, and
  - The payer is not in an abnormal location, and
  - The payer is not in a high-risk location.

ETV	Reference Fraud Rate (%) for	
	Remote Electronic Card-Based Payments	Remote Electronic Credit Transfers
€500	0.01	0.005
€250	0.06	0.01
€100	0.13	0.015

In addition, PSPs wishing to use TRA as an exemption to SCA must at least take into account risk factors such as previous spending patterns, payment transaction history, correlation between spending pattern and transaction history, and location of both payer and payee at the time of the transaction.

Essentially, the regulation mandates risk-scoring for each transaction and if the risk is low and an exemption applies, SCA will be not required. This means that frictionless payment methods (e.g. one-click) are still possible, but ecosystem players must be able to use data effectively to ensure they assess their risk correctly. The best solutions will be those that enable entities to use data effectively and quickly to derive actionable insights to prevent fraud and cybercrime in our fast moving digital world.

Kaspersky®
Fraud Prevention

More information: kaspersky.com/fraudprevention

Kaspersky Lab HQ Office
39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

info@kaspersky.com
kaspersky.com
kfp.kaspersky.com
#truecybersecurity