Revised Payment Services Directive sets the stage for retail banking in 2018

Raili Liiva
Sales and Market Research
Messente Communications, Ltd.

At the beginning of 2018, European Union member states will be required to implement the second Payment Services Directive (PSD2.)[1] The Directive aims to improve the payment industry and its services across Europe. Since the introduction of the first Payment Services Directive in 2007, developments in technology led to new forms of payment services entering the market, such as internet and mobile banking, peer-to-peer applications, and e-wallets[2].

The new law builds on the legislative framework established by the original directive. PSD2 acknowledges the rise of payment related financial technology companies (fintech) and it creates equity amongst all payment services providers, while ensuring improvements in security and stronger customer protection. All payment service providers and digital currency issuers are affected, including businesses currently not authorized or registered with the Financial Conduct Authority, yet execute payment related activities.

[1] Financial Conduct Authority – Implementation of PSD2
[2] Financial Conduct Authority – Revised Payment Services Directive

Comparing PSD and PSD2

What's new in PSD2?

01
Reach expands outside of the EU, affecting payment service providers that do business with EU residents.

02
Banks required to open access to data to 3rd party technology providers.

03
Fees to customers cannot exceed actual costs.

04
Authentication improvements require multi-factor authentication.

05
Payment service providers required to indemnify customers in the event of fraud within a day.

Geographical Scope

The second version of the Directive significantly increases the geographical reach of regulations. Under PSD1, transparency and conduct of business requirements applied only to transactions where the payment service provider (PSP) for both the payer and recipient was in the EU. PSD2 expands original PSD rules to transactions in which at least one party of the transaction is located within EU borders.

Competition, New Solutions, More to Regulate

PSD2 rules increase competition and encourages market participants to innovate, which is positive for consumers, yet it adds players to be regulated. It encourages new players to enter the payment market by mandating banks to provide access to the systems behind bank accounts to external parties, like Account Information Service Providers (AISP) and Payment Initiation Service Providers (PISP,) both of which must now comply with PSD2.

- AISPs connect to bank accounts and retrieve information. For example, it allows information from multiple accounts to be pooled into one portal for viewing. Personal finance management tools and online investment advisors use these providers to build their platforms (like the tools from Mint.com.)
- PISPs initiate payment transactions. Currently there are only SEPA Credit Transfers and debit cards in the EU. Peer-to-peer applications and bill payment services are PISP services likely to rise after PSD2 is implemented.

PSD2 obligates banks to give third-party technology providers access to their customers' accounts through open application program interfaces (API,) allowing third parties to build financial technology services on top of banks' data and infrastructure[3]

The mandate creates an opportunity for major technology firms to further proliferate in the payments industry in Europe. Companies like Apple, Google, and Facebook are expected to take advantage of the new legislation. While still speculative, it will be interesting to see how major tech firms will react.

Surcharging for Payments

Current bank practices regarding surcharges vary by EU member; a few countries ban it, others do not. PSD2 prohibits charging a customer fees that exceed the direct cost of the payment instrument, a cost that must be published for customers to view.

Improve Strong Customer Authentication

With high-profile hacks proliferating across varying industries, PSPs must ensure that security measures are in place to protect the confidentiality and integrity of personalized security credentials. Article 97 of PSD2 requires payment service providers to authenticate users when 1) accessing an online payment account, 2) initiating an electronic payment transaction, and 3) carrying out an action through a remote channel that may imply a risk of payment fraud or other abuses[4].

[3] European Banking Authority - Guidelines on securing measures for operational and security risks under the PSD2

[4] European Banking Authority - Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

Core Considerations: Fraud and Security

The implications of the law center around the consumer and their rights[5]. Section 73 of PSD2 protects consumers and forces indemnification.

> "...in the case of an unauthorized payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorized payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction."

This rule also applies to unauthorized transactions done through a PISP.

Payment firms and intermediaries must prioritize client data security when building their systems.

The basic definition of "strong customer authentication" is presented in article 4(30) of PSD2. It states that authentication must be based on the use of *two or more possible authentication elements*, categorized as:

- Knowledge (i.e., something only the users knows, such as a password)
- Possession (i.e., something only the user has, such as a token or device)
- Inherence (i.e., something only the user is, which a fingerprint or a face scan proves)

Furthermore, Article 98 grants the European Banking Authority the responsibility to develop Regulatory Technical Standards (RTS) for strong customer authentication. The process of creating the standards involved discussions and over 250 comments from different parties. The final draft of the RTS was published in February 2017 and sent to the EU Commission for confirmation[6].

Briefly, the RTS creates requirements around the application of two-factor or multifactor authentication in the context of PSD2. The requirements will apply 18 months after the EU Commission confirms the standards. If they are confirmed in October 2017, organizations impacted by PSD2 would need to comply around April 2019[7].

[5] Revised rules for payment services in the EU
[6] Regulatory Technical Standards on strong customer authentication and secure communication under PSD2
[7] EBA mandates in PSD2 and their timelines

2FA: Security vs. Customer Experience

Consider the following

01
Mobile phones establish a 'known' object for 2FA

02
80% of EU citizens in advanced economies use smartphones

02
SMS 2FA ubiquitous in the majority of Europe, not requiring a network connection

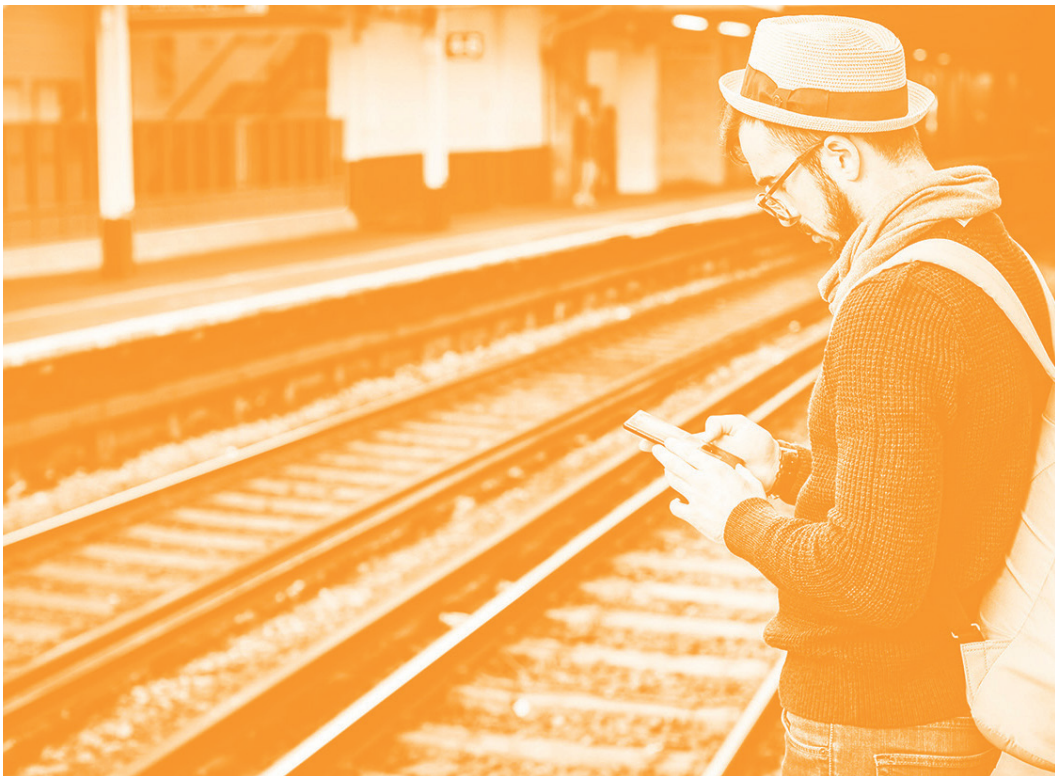
04
Payment information must transfer to 2FA source securely.

Friction between creating superior user experience and providing high-level security has always existed. However, proliferation of mobile phones created an opportunity for secure mobile authentication, while developing convenient technology.

60% percent of EU citizens use network-connected mobile devices (smartphones,) with over 80% of citizens in nations of the EU with more advanced economies using smartphone[8]. These figures do not consider non-network-connected devices that receive SMS messages (which work in rural areas of Europe where mobile data networks have not yet been built.)

Mobile phones establish a 'known' object that consumers possess, creating a method for two-factor authentication. New smartphone models also contain biometric security features, like fingerprints and facial recognition. These methods allow regulated financial organizations to accurately verify the identity of a user requesting access.

However, there are additional considerations to selecting a solution.



[8] EuroStat – Digital Economy and Statistics

Mobile app

As the mobile app that generates the PIN code must also show the payment information to the user, described in PSD2 rules, the payment service and authentication app must exchange payment information via a secure channel. It should also be equipped with security software that can detect malicious software, preventing it from interfering with the payment transaction.

SMS

The SMS messages used for authentication must also contain payment information. The requirement to protect the confidentiality of the payment information could be interpreted as a need to encrypt the payment information in the SMS message. However, more clarification on this subject should be available after the final draft of the RTS is confirmed.

SMS vs STOTP*

SMS

01
No network connection required

02
Simple to use – no user app needed

03
Reaches more people (no need for a smartphone)

04
Less secure due to SS7 vulnerabilities

05
Must encrypt payment data

TOTP

01
App download required

02
One-time password will work with no data connection

03
Network needed to pass payment data

04
More secure as PIN code data never transmitted

*Time-based one-time passwords are PIN codes that expire in a certain time frame, typically 30 seconds. Commonly known as tokens, these PIN codes are synced with the corresponding server when 2-factor authentication is set up with an online service. The PIN is never transmitted through the data network and will work without a data connection.

Conclusion

Undoubtedly, uncertainty exists for banks and fintech firms. It is not certain how the industry will react once the regulations are enforced; however, they must plan to make changes to processes and policies. Lastly, while PSD2 establishes new rules regarding the data available to third parties and security, the General Data Protection Regulation (GDPR) creates new definitions and enforcement to privacy. Creating systems and processes that comply with both laws is crucial and selecting the right partners help organizations through the journey.

Sources

"Payment Services Directive: frequently asked questions." *European Commission - PRESS RELEASES - Press release - Payment Services Directive: frequently asked questions*, europa.eu/rapid/press-release_MEMO-15-5793_en.htm

"Revised Payment Services Directive (PSD2)." *FCA*, 27 Sept. 2017, www.fca.org.uk/firms/revised-payment-services-directive-psd2

"Implementation of PSD2." *FCA*, 19 Sept. 2017, www.fca.org.uk/firms/revised-payment-services-directive-psd2/implementation

"Regulatory Technical Standards on strong customer authentication and secure communication under PSD2." *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 - European Banking Authority*, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

"Guidelines on security measures for operational and security risks under the PSD2." *Guidelines on security measures for operational and security risks under the PSD2 - European Banking Authority*, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

"Guidelines on major incidents reporting under PSD2." Guidelines on major incidents reporting under PSD2 - European Banking Authority, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

"Guidelines on authorisation and registration under PSD2." *Guidelines on authorisation and registration under PSD2 - European Banking Authority*, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2/-/regulatory-activity/press-release

"FINAL REPORT ON GUIDELINES ON AUT HORISATION AND REGISTRATION UNDER PSD2." European Banking Authority.

Revised rules for payment services in the EU, eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM%3A2404020302_1&from=EN&isLegissum=true.

"EBA OPINION ON EC PR OPOSED AMDENMENTS TO RTS ON SCA AND CSC U NDER PSD2." European Banking Authority.

"EBA publishes final Guidelines on authorisation and registration under PSD2." *EBA publishes final Guidelines on authorisation and registration under PSD2 - View press release - European Banking Authority*, www.eba.europa.eu/-/eba-publishes-final-guidelines-on-authorisation-and-registration-under-psd2

"EBA mandates in PSD2 and their timelines." European Banking Authority.

"Guidelines on fraud reporting under PSD2." *Guidelines on fraud reporting under PSD2 - European Banking Authority*, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

"Regulatory Technical Standards on strong customer authentication and secure communication under PSD2." *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 - European Banking Authority*, www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

"FINAL REPORT ON DRAFT RTS ON SCA AND CSC ." European Banking Authority, 23 Feb. 2017

"Digital economy and society statistics - households and individuals." *Digital economy and society statistics - households and individuals - Statistics Explained*, ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals