Future of Payments

Challenges for banks: e-wallets and the application of strong customer authentication

Jan Jans,
Partner, RegCounsel Financial Services

ABSTRACT

The digitalization of payments has elevated the role of technical service providers (TSPs), such as e-wallet providers, in the client-facing layer of the payment chain. Their growing involvement poses challenges for card-issuing banks, particularly regarding their obligation to apply strong customer authentication (SCA) under the Revised Payment Services Directive (PSD2). This article argues that TSPs involved in the authentication process act as outsourced service providers for the purposes of SCA, triggering compliance with the broader outsourcing framework - including the EBA Guidelines on Outsourcing and DORA. As TSPs are not typically subject to direct supervision by financial regulators, banks may struggle to enforce the contractual safeguards required by outsourcing rules. This tension raises questions about enforcement and accountability in the current regulatory architecture.

1. Introduction

In the past decades, the digitalization of the European retail payment market has resulted in a significant increase in the development of new and innovative payment products, including the introduction of contactless payment methods [E.U. (2023)]. While payment products were initially primarily offered by banks, non-regulated service providers are increasingly taking part in the payment chain. Some of these service providers develop client-facing interfaces that enable payment service users (PSUs) to use their bank issued debit or credit cards to make payments. For example, BigTechs, such as Apple, Google, and Samsung, offer digital wallets that are used by PSUs to make contactless payments with tokenized debit and credit cards using the Near Field Communication (NFC) chip installed on their smartphone (e-wallets). The services offered by e-wallet providers are typically in support of the payment services offered by banks and do not in themselves qualify as regulated payment services, as described by PSD2, as these e-wallet providers are never in possession of the funds that are transferred. Consequently, these service providers, also referred to as technical service providers (TSP) under PSD2, are not required to obtain payment service provider (PSP) licenses and are, therefore, not subjected to the PSD2 framework.

With the increasing participation of unregulated service providers in the payment chain, banks are facing additional challenges when trying to safeguard the security of their electronic payment offerings. In addition to adding layers of complexity to the payment process, banks are also facing additional challenges when trying to meet their own legal obligations. One area where this is causing concern for banks is the undertaking of strong customer authentication (SCA) while having to rely on the e-wallet providers even though they are not mandated to undertake such authentication by PSD2.[1]

In June 28, 2023, the European Commission (Commission) published a proposal for a payment services regulation (PSR Proposal) as part of the Financial Data Access and Payments Package,[2] which, amongst others, aims to strengthen PSU protection as well as the confidence in the use of payment products by introducing improvements to the application of SCA involving e-wallets. The PSR Proposal was amended by the European Parliament (EP) on April 23, 2024 (EP Amendment) and by the Council of the European Union (Council) on June 13, 2025 (Council Amendment) and has entered the trilogue negotiations at the moment of writing.

This article analyses the proposed amendments to the PSD2 SCA requirements for banks in the context of e-wallets under the PSR Proposal, thereby taking into account the practical challenges banks are facing as a result of their interactions with TSPs offering e-wallets.

2. Strong customer authentication (SCA) under PSD2

When a bank receives a payment order from a PSU, the PSD2 authentication obligation requires it to verify the identity of the PSU and the use of the payment instrument by the PSU (Article 4(29) PSD2). SCA is an enhanced form of authentication that requires a combination of at least two authentication elements categorized as knowledge, possession, and inherence (Article 4(30) PSD2). The "knowledge" element relates to information that only the PSU has (e.g., PIN code or password). The "possession" element refers to something that only the PSU possesses (e.g., a random reader or a smartphone). The possession element does not have to be something physical but can also be non-physical such as an app, provided there is a unique connection between the possession element and the PSU [EBA (2020)]. The "inherence" element reflects something that the PSU is (e.g., fingerprint scanning, facial recognition, or behavioral biometrics) [EBA (2019a)]. For online card payments, the technology most used by banks to conduct SCA is 3D Secure,[3] which involves a security protocol to confirm the PSU's identity using, for example, the PSU's fingerprint [E.U. (2023)].

1. It should be said that while they are not covered by PSD2, e-wallet providers are subject to the Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA) as part of their role as "arrangement providing functionalities supporting the use of electronic payment instruments".
2. Further to the PSR Proposal, the Financial Data Access and Payments Package also includes a proposal for the Third Payment Services Directive (PSD3) and a Financial Data Access (FiDA) Regulation.
3. 3D Secure was introduced in 2018 by EMVCo, which is a consortium between Visa, American Express, Mastercard, China UnionPay, Discover, and JCB.

The two elements used for the SCA process must be mutually independent, meaning that a security breach of one element should not result in a breach of the other element.[4] The requirement that the authentication elements must be mutually independent means, according to the European Banking Authority (EBA) PSD2, that the two elements have to belong to two different categories [EBA (2020)].

A valid combination of two authentication elements results in the generation of a unique authentication code, which is accepted only once by the bank for the execution of a payment (Art. 4(30) PSD2 jo. art. 4(1) Delegated Regulation (EU) 2018/389). In the event that SCA is applied for a so-called remote payment (i.e., payment initiated via the internet or a device for distance communication), the bank must apply dynamic linking, which involves the generation of a unique authentication code specific to both the transaction amount and the identity of the beneficiary) (Article 97(2) PSD2.). It should be noted that even contactless payments via a QR code qualify as remote payment transactions because they are initiated via the internet, and, therefore, require dynamic linking as part of SCA.

2.1 When is strong customer authentication (SCA) required?

PSD2 requires banks to apply SCA in the event that the PSU: (i) accesses its payment account online, (ii) initiates a payment in the capacity as payer,[5] (iii) creates a list of trusted beneficiaries (i.e., businesses assigned by the PSU to a whitelist of trusted beneficiaries), or (iv) carries out an action through a remote channel which may imply a risk of payment fraud (Article 97(1) PSD2).

In order to help with the development of user-friendly and low-risk payment services, banks are allowed to disapply SCA in certain circumstances (Recital 11 Delegated Regulation (EU) 2018/389). For example, an acquirer can request that the bank applies a transaction risk-based exemption for SCA for low-risk transactions if the acquirer's or bank's fraud rates are below certain thresholds (Article 18 Delegated Regulation (EU) 2018/389). Furthermore, in order to establish some kind of balance between enhanced security and user-friendliness in remote payments, the bank can decide to disapply SCA for remote low value payments (i.e., transactions that do not exceed €30), provided that the total transaction amount initiated with a particular payment instrument since the last time SCA was applied does not exceed €100 and that there have not been more than 5 consecutive transactions since the last application of SCA (Article 16 Delegated Regulation (EU) 2018/389). Banks can also choose not to apply SCA for recurring fixed-amount transactions from the second transaction onwards, provided that the beneficiary and the transaction amount do not change (Article 14 Delegated Regulation (EU) 2018/389).

It is important to note, however, that the decision not to apply SCA is not risk free, since under PSD2 the bank remains liable for any unauthorized transaction, unless the payer has acted fraudulently (Article 74(2) PSD2).

3. E-wallets and the obligation to conduct strong customer authentication (SCA)

With an e-wallet, the PSU can use its bank-issued payment instrument (e.g., debit- or credit card) to make online or contactless payments (i.e., remote payments) via its smartphone through a process called tokenization [E.C. (2023a)]. Tokenization involves the replacement of the PSU's primary account number (PAN) with a unique algorithmically generated number referred to as the payment token (Token).[6] According to the Commission, the Token itself is not to be considered a "payment instrument "within the meaning of PSD2 but merely a "payment application" within the meaning of article 2(21) of the Interchange Fees Regulation [E.U., 2015)] (Recital 24 PSR Proposal). According to EBA, the Token can qualify as a "possession element" for SCA purposes provided that the card issuer is involved in the issuance of the Token [EBA (2020)]. A PSU that wishes to use an e-Wallet for making payments, must first add one of its payment instruments to its e-wallet.

4. Article. 9(1) Delegated Regulation (EU) 2018/389. If a PSU uses a multipurpose device for conducting SCA, such as a smartphone, article 9(3) Delegated Regulation (EU) 2018/389 requires the PSP to use separated secure execution environments via the software installed on such device.
5. SCA is required for online European payments. This means both the merchant's and cardholder's Bank are established in Europe.
6. The main difference between tokenization and encryption is that with tokenization the original data cannot be recovered from the Token.

3.1. Adding a payment instrument to an e-wallet

When a PSU adds a debit or credit card to its e-wallet, the card details (including the PAN) are shared with the TSP offering the e-wallet, which subsequently identifies the bank who issued the respective card. Upon receipt of the PAN related to the card that is to be added to the e-wallet, the bank requests a so-called token service provider, such as Visa Token Service or American Express Token Service, to issue a Token for the relevant card. Both the Token and PAN are stored by the token service provider and the Token is shared with the bank. Subsequently, the Bank shares the Token with the TSP offering the e-wallet, which stores the Token in the secure element of the PSU's smartphone (secure element).[7]

The process of tokenization, where the PAN is replaced by a Token, is considered by PSD2 to constitute an "action through a remote channel which may imply a risk of payment fraud or other abuse," which means that if a PSU adds a card to its e-wallet, the card issuing bank is obligated to conduct SCA as part of this process. In fact, Article 85 of PSR Proposal explicitly states that SCA must be applied at the moment of a Token creation or replacement. Consequently, the PSU is directed to the online interface of the bank to complete SCA before the bank requests the token service provider to issue the Token.

3.2. Initiating a payment with a tokenized card

If a PSU wishes to initiate a payment via its e-wallet, the "authentication" obligation under PSD2 requires the bank to verify the identity of the PSU (also referred to as customer authentication) as well as the details of the transaction (also referred to as transaction signing) (Article 4(29) PSD2). With ordinary card payments, these processes are both completed by the card issuing bank, whereas with e-wallets, customer authentication takes place within the e-wallet interface instead of the bank's interface. In other words, if a payment is initiated with an e-wallet, it is the TSP, rather than the bank, who verifies the identity of the cardholder.

Thereafter, the Secure Element generates a cryptogram for the transaction, which is based on the transaction information and Token. The cryptogram is sent together with the transaction information and Token to the acquirer via the merchant's Point of Sale (PoS) device. The cryptogram and Token are then sent to the card network, which validates the cryptogram and de-tokenizes the Token. Subsequently, the card network sends the PAN and transaction data to the bank, which is responsible for the verification of the payment instruction initiated with its card (i.e., the transaction signing) and the transfer of the corresponding funds to the acquirer.

3.3. Interplay between the bank and TSP

Given that under PSD2 the bank is responsible for both customer authentication and transaction signing, the question arises as to whether the customer authentication conducted by the TSP as part of an initiated payment via an e-wallet qualifies as the outsourcing of an element of the SCA requirement to the TSP [Jans (2024)].

Given that the bank receives confirmation from the TSP that the PSU's identity has been verified instead of the bank actually verifying its identity, the bank relies on the correctness of input provided by the TSP in order to complete the "authentication process".

In my opinion, the involvement of the TSP in the authentication process constitutes outsourcing, as outlined by the regulatory framework, which means that the bank must comply with numerous legal requirements applicable to outsourcing arrangements, in particular if the involvement of the TSP constitutes critical outsourcing.

This implies that the bank will not only be required to meet the outsourcing requirements under the EBA Guidelines on outsourcing [EBA (2019b, 2025)] but also the outsourcing requirements imposed under the Digital Operational Resilience Act (DORA).[8] For example, the bank will have to ensure adequate oversight of the performance of the TSP's outsourced functions and enter into an outsourcing agreement with the relevant TSP that

7. For example, iPhones have a "secure element" in their NFC chip where the Token is stored. The PAN is never stored on the device.
8. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. DORA forms part of the broader Digital Finance package of the Commission and seeks to bring harmonization of the rules relating to operational resilience for the financial sector. The European Supervisory Authorities (ESAs) are currently preparing to designate critical third-party service providers (CTTSP) under DORA. Given the important role of certain TSPs in the SCA process, it is likely that (some of) these TSPs will be designated as CTTSP under DORA.

allows the bank to have a certain level of control over the outsourced function, such as the bank's audit rights. Before signing such an agreement, DORA requires the bank to conduct a thorough risk assessment, which includes, amongst others, an assessment of operational, legal, ICT-related, reputational, and data protection risks. If the TSP does not meet the agreed key performance indicators (KPIs) and no other remedy is available, the bank must either transfer the outsourced function to a third party or conduct this process itself.

Given that the current PSD2 framework does not explicitly consider such TSP involvement as outsourcing, legal outsourcing requirements have typically not been made part of any contractual arrangement between banks and TSPs offering e-wallets. Offering e-wallet solutions, therefore, gives rise to regulatory concerns since banks are not able to apply any controls or checks on the security measures and their compliance with the requirements of PSD2, Delegated Regulation (EU) 2018/389 and DORA. Moreover, given that the PSD2 framework for SCA is not directly applicable to TSPs, there is no regulatory incentive for TSPs to assist the banks in meeting their regulatory obligations.

4. The PSR Proposal

In its evaluation of PSD2, the Commission concluded that the application of SCA by PSPs has been very successful in reducing payment fraud (Recital 107 PSR Proposal). This view is also supported by other evaluations, such as the joint report on payment fraud in the European Economic Area published by the EBA and the European Central Bank in August 2024 [EBA/ECB (2024)]. Although the security of payment transactions has improved as a result of the SCA requirement, the Commission's evaluation also shows that the obligation to conduct SCA has made the customer journey for certain PSUs more difficult [E.C. (2023b)]. For example, the fact that there is still a significant number of PSUs who do not, or cannot, use smartphones for online and contactless payments imposes barriers for these persons to complete the SCA process. To improve financial inclusion, the Commission, therefore, stresses, in line with the European Accessibility Act [E.U. (2019)], the importance of banks facilitating all PSUs, including those who do not have access to digital devices such as smartphones, to benefit from protections against fraud that are provided by SCA [E.C. (2023a)].[9]

Generally, however, the use of the smartphone as part of the SCA process has taken a prominent role in the payment chain. With the increasing use of e-wallets by PSUs and the lack of a clear legal framework covering the interplay between banks and TSPs, the Commission considered it essential to address TSP involvement in the SCA process in the PSR Proposal [E.C. (2023a)]. The Commission takes the view that the involvement of e-wallet providers in the SCA process constitutes outsourcing and that such TSPs should, therefore, be subject to the legal requirements covering outsourcing arrangements by PSPs. Although the Commission recognizes the importance of TSPs as part of the payment chain, it does not want to go as far as bringing these service providers within a PSP license regime at this point in time [E.C. (2023a)].

4.1. E-wallets and the outsourcing of part of the SCA process

The Commission suggests in the PSR Proposal that TSPs that verify elements of the SCA will be required to enter into outsourcing agreements with the banks regarding their involvement in the SCA process, and liable for failure to support the application of SCA (Article87 PSR Proposal). As with outsourcing in general, it is explicitly mentioned in the PSR Proposal that in case of outsourcing the bank remains fully liable *vis-à-vis* the payer for any failure to apply SCA (Article 87(2) PSR Proposal). To ensure that this legal obligation can be enforced in practice, the Commission suggests that the competent authorities overseeing compliance with the payments framework shall have the power to require all the information from TSPs that it considers necessary to carry out any investigation of potential breaches of the law (Article 91(5) PSR Proposal). The PSR Proposal does not, however, seem to allow competent authorities to also impose administrative measures or sanctions on TSPs in case of a breach of law.

The EP appears to take a different view regarding the qualification of TSP involvement in the SCA process given that the requirement for the bank to have an outsourcing agreement in place with the TSP has been deleted in the EP Amendment.

9. According to Recital 110 PSR Proposal, PSPs must ensure that their customers can benefit from various methods to perform SCA which are adapted to their needs and situations, which should not depend on one single technology, device or mechanism, or on the possession of a smartphone or another smart device.

This deletion has, however, been reversed by the Council, which suggests that there is a lack of agreement between the European institutions on how to best address this topic (Article 87(1) Council Amendment). It remains to be seen which position will make it to the final text of the PSR Proposal after the trilogue negotiations.

Further to the legal qualification of TSP involvement in the SCA process, the Commission takes the view that the TSP is to be held liable in case of failure to support the SCA process. To this end, the Commission included in the PSR Proposal that TSPs offering e-wallets are to be held liable for failure to support the application of SCA *vis-à-vis* the bank within the remit of their contractual relationship (Article 58 PSR Proposal). Although the EP does not require the bank and the TSP to enter into an outsourcing agreement, it does maintain this liability provision, albeit with the limitation that the TSP is only to be held liable in these circumstances for "direct" financial damages whereby the liability should be proportionate to the shortcoming and the amount of the transaction (Article 58 EP Amendment). It strikes me as odd that the EP does not recognize the TSP involvement as outsourcing and at the same time wants to hold the TSP liable if it falls short in its involvement in this process. In line with the Commission, the Council suggests to broaden the scope of the TSP's liability by stating that the TSP is to be held liable for "any financial damage" rather than "direct financial damage" (Article 58 Council Amendment). Furthermore, the Council aims to make this requirement directly applicable to TSPs under the Council Proposal (Article 1a PSR Proposal).

It is also helpful for banks that from a competition law perspective steps have been taken regarding third party access to the NFC antenna installed on smartphones. On March 19, 2025, the Commission ruled that Apple, acting in the capacity of "gatekeeper" under the Digital Markets Act (DMA) [E.U. (2022)], must open up iOS connectivity features to third-party devices [E.C. (2025)]. Initially, smartphone producers that also operate as e-wallet providers did not provide third-party access to these devices, which meant that banks could not develop their own e-wallet solutions to be installed on a smartphone. Furthermore, because of the lack of access, banks were not able to transfer the outsourced SCA process to themselves or another service provider if the KPIs were not met by the e-wallet provider that also produced the smartphone on which the e-wallet is installed. With the Commission's decision, an important step is made to help banks meet their legal obligations when their cards are being used for making payments via an e-wallet.

5. Conclusion

With the further digitalization of the payments market, TSPs offering e-wallets have acquired a prominent role in the payment chain. It has, therefore, become even more important to have clear rules on the interplay between card issuing banks and TSPs when it comes to TSP involvement in the SCA process.

With the PSR Proposal, the Commission has taken an important step towards recognition of the role of e-wallet providers and the legal challenges that they impose on banks under the PSD2 framework. Although the EP appears to take a different view, the Commission and Council clearly recognize the involvement of these service providers in the SCA process as outsourcing by the card issuing bank. This means that the bank is obligated to implement the legal outsourcing requirements *vis-à-vis* the TSP, which is currently difficult given that PSD2 does not explicitly recognize this legal qualification and does not impose any requirements in this regard on TSPs. Although I welcome the steps that are suggested by the Commission and the Council with the PSR Proposal, these amendments do not, in my view, fully take away the practical challenges that banks face in this regard. Although the outsourcing requirements should theoretically be complied with when the bank and TSP have an outsourcing agreement in place, the fact that the competent authorities supervising the payments sector cannot impose enforcement measures or administrative sanctions on TSPs regarding their involvement in the payment chain, may in practice result in a lack of incentive for these TSPs to ensure that individual banks can comply with the regulatory framework. In practice, this means that it is not unlikely that individual banks may encounter difficulties in agreeing on the required documentation with TSPs, in particular when these TSPs have a dominant market position. The fact that the Council suggests to explicitly apply the PSR outsourcing requirements to TSPs does not, in my view, alter these practical concerns given that the Council Amendment does not seem to allow competent authorities for the payments sector to impose enforcement measures or administrative sanctions on TSPs in case of a breach of law.

Although it remains to be seen how the Digital Markets Act (DMA) and the critical third-party service providers (CTTSP) designations by the ESAs under DORA will impact compliance by TSPs with these requirements, it might help to consider the option of bringing TSPs that support the authentication process within the remit of supervision by these competent authorities, even if it is merely a registration requirement. Better supervision of TSP compliance with the outsourcing requirements could in my view be provided for when these TSPs are brought under the supervision of the competent authorities for the payments sector.

References

EBA, 2019a, "EBA publishes an Opinion on the elements of strong customer authentication under PSD2," European Banking Authority, June 21

EBA, 2019b, "Final report on EBA Guidelines on outsourcing arrangements," European Banking Authority, EBA/GL/2019/02, February 25

EBA, 2020, "Strong customer authentication and common and secure communication (incl. access)," European Banking Authority, July 24

EBA, 2025, "The EBA launches consultation on its draft Guidelines on third-party risk management with regard to non-ICT related services," European Banking Authority, July 8

EBA/ECB, 2024, "The EBA and ECB release a joint report on payment fraud," European Banking Authority and European Central Bank, August 1

E.C., 2023a, "On the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market," European Commission, June 28

E.C., 2023b, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)," European Commission, February 2

E.C., 2025, "Commission provides guidance under Digital Markets Act to facilitate development of innovative products on Apple's platforms," European Commission, March 19

E.U., 2015, "Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance)," European Union, April 29

E.U., 2019, "Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance)," European Union, April 17

E.U., 2022, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)," European Union, September 14

E.U., 2023, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)," European Union, FISMA/2021/OP/0002

Jans, J. A., 2024, Electronic payments in the European market: creating a level playing field between banks and non-banks, EBI Studies in Banking and Capital Markets, Palgrave Macmillan