Do TPP Services Represent a Worrying Factor for The Retail Payments Market?

An SPA Paper

November 2019

Introduction

The revised Payment Services Directive (PSD2), along with the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under PSD2 (The RTS on SCA), establishes a legal framework intended to enhance competition in the European Economic Area (EEA) retail payments market. However, this increased level of competition must not be achieved at the cost of additional payment fraud. This is one reason why the PSD2 further protects end-users by mandating the use of Strong Customer Authentication (SCA) for payments and online banking.

SCA applies to a large diversity of payment instruments in the Single European Payment Area (SEPA) implemented using different form factors - ranging from debit/credit cards to Internet of Things (IoT) networks. However, because the PSD2 and the RTS on SCA are legal texts, they are not prescriptive on the specific technologies required to implement SCA. Following the RTS on SCA publication in March 2018, the European Banking Authority (EBA) has been releasing annual Opinions designed to address this gap. Needless to say, these are highly controversial in the payments industry at large.

Other than SCA, the PSD2 also mandates that banks provide a dedicated interface so identified Third Party Payment Providers (TPPs) can gain access to customer payment account information and initiate payments on their behalf. This dedicated interface is usually implemented as an Application Programming Interface (API). SCA must also be implemented whenever a payment is initiated by the TPP using this API. The point here is that deploying convenient SCA methods when a TPP is involved is challenging. If the SCA methods are not adapted to the TPP context, it is likely that the PSD2 fails.

In this paper SPA investigates the new market context created by the PSD2, globally known as Open Banking, from four different angles:

1. The impact of TPPs on the structure of the retail payments market should the TPP model succeed
2. The security risks of Open Banking and how card technology may mitigate these
3. The implementation of SCA in a TPP context
4. The functional and security standardization of Open Banking and the SPA's role enabling role.

This paper details the SPA positions with regards these four issues and suggests ways to move ahead. NOTE: In this document, the term *customer* refers to bank customer. The term *consumer* refers to the same person acting as a purchaser or a client of the retailer.

TPP Financial Services Regulated by the PSD2

The PSD2 regulates the payments market with respect to three types of services that may be offered by non-banks:

1. Payment Account Aggregation provided by a TPP named Account Information Service Provider (AISP)
2. Payments provided by a TPP named Payment Initiation Service Provider (PISP)
3. Card payments using a card not issued by the bank holding the account that the card is associated to. This point is addressed in the paper in a specific clause: Integrating the card in the Open Banking context.

Depending on the business model, a TPP might play any combination of the above roles. For instance, an account information transaction (to know the amount available in a bank account) could be a prerequisite to initiate a payment with that account. The TPP is likely to be the same for both consecutive services. Yet the business opportunities for Fintech are perceived to be more in the area of capturing and consolidating payment account information, rather than in the area of initiating payments. Because account information services do not require the transfer of funds, there is no direct risk to the cardholder's account. Therefore, those TPPs acting as AISPs argue that there is no reason to restrict the number of times that the API can be accessed for that purpose.

The PISP is expected to agree on a business arrangement with a retailer for the provision of Payment Initiation services. The PSD2 sets out that the PISP cannot hold the funds to be transferred at any time during the transaction. Therefore, a new business case is needed for the PISP – where the fee charged to the retailer is lower than the one charged by the acquiring bank when payments are made by card. At present, SEPA (instant) credit transfers are considered the only realistic option for payments initiated by a PISP, and card payments are not a real option. However, card payment technology is appropriate for strong customer authentication purposes and could be used for non-card based SEPA payment instruments, such as a credit (instant) payment. The next section provides additional insight into the TPP authentication challenges and the different trade-offs to be considered when deploying authentication solutions.

SPA's opinion is that the authentication methods that are applied in a TPP context will impact the final success of the Open Banking ecosystem and its potential to change retail payment market structures.

PSD2 and RTS on SCA Implementation:

Where We Are Today

The TPP business model is not new: Sofort in Germany and Ideal in the Netherlands were both successful TPP organizations prior to the PSD2 publication. Yet, following the implementation of PSD2, TPPs have become regulated and must apply for a license granted by an EEA competent authority to gain access to customer data using the bank API. This obligation for the banks to share customer data with TPPs is viewed by the payments industry as a disruptive event. In this paper, the term Open Banking is used whenever referring to this new scenario.

The Open Banking ecosystem will be hard to manage because the multiplicity of actors/roles involved all have strong conflicts of interests. The TPP role may (and will) also be played by individual banks or a bank consortium – and not just by the well-established TPPs or incomers such as FinTechs, or even GAFA (Google, Apple, Facebook and Amazon). International card schemes also intend to provide Open Banking services, even if the TPP privileged payment instrument is the SEPA (Instant) Credit Transfer. Finally, big overseas players – such as Alibaba – are now signing bilateral contracts with local payment service providers to position in this market.

Simultaneously, according to the same regulatory framework, banks must provide Personal Security Credentials (PSCs) to their customers for Strong Customer Authentication. SCA applies when the customer is paying in a physical shop or online, but online payments will require the generation of a specific code with dynamic linking, i.e. with transaction signing. To preserve the user experience, the RTS on SCA sets out a limited exemption regime that will apply to certain scenarios – such as low value contactless and online payments, tolls and parking payments, or transactions categorized as low risk.

It is important to point out that the consumer must be equally protected when accessing their own bank payment account directly – whether using a mobile application provided by the bank, or via a TPP. This means that the same Personal Security Credentials should also be used when the user starts interacting with a TPP. This legal requirement is challenging from an implementation perspective and the issue is explored in more detail below.

Because the law is expected to be technology-agnostic, neither the PSD2 nor the RTS on SCA provided details for implementation. This original gap is now being closed by two initiatives:

- **The Opinions released annually by the European Banking Authority (EBA) for PSD2 implementations.** In principle, these are not legally binding. However, the EBA has been empowered following the recent reorganization of responsibilities between the different EU regulatory authorities – Eurosystem, the European Commission Directorate-General (DG) for Competition, and the Directorate General (DG) for Financial Stability, Financial Services and Capital Markets Union (FISMA). In its last Opinion, released in June 2019, the EBA provides definitive statements on which authentication elements are eligible to implement Strong Customer Authentication according to the PSD2. In past position papers SPA has highlighted why not all authentication elements - regardless of their category – are equal from a security perspective. The EBA Opinion states that the PSD2 elements used for authentication must effectively identify the customer, and highlights that while collecting data about a transaction's context can help to evaluate risk – it does not eradicate it.
- **Standardization at national (especially), European (partially) and international levels, such as the International Standardization sub-committee for banking, securities and other services (ISO TC68) and the Fast Identity Online (FIDO) Alliance.** Deeply involved in assessing and participating in all these standardization initiatives, SPA believes that standards represent the first line of defense for preventing excessive market fragmentation and eliminating sources of security issues. Standards promoting the use of a high level of security for implementations are the best way to preserve the integrity of the customer payment account.

SPA also observes that a number of overseas countries are now using the PSD2 model to set out their own regulatory frameworks and incentivize Open Banking. As in the EEA, these regulatory

frameworks attempt to reconcile a more competitive retail payments market without adding vulnerabilities. SPA considers that SCA is a good approach, provided that the hardware and software authentication components used for SCA are reliable.
The issue remains, however, that the replacement of existing authentication elements with those prescribed by the EBA requires a considerable investment effort by both the banking industry and retailers at a time when both sectors are contending with a complex economic backdrop. Not surprisingly, the European Association of Payment Service Providers for Merchants has released a paper position objecting to the positions expressed in the June 2019 EBA Opinion, requesting a further 18-month extension to achieve conformance with the RTS on SCA.

1. The Impact of Open Banking on Retail Payments Market Structures

Euro Area Banking Sector: The Economic Context

The persistently weak profitability of the Euro area banking sector in the post-financial crisis era is constraining its ability to build liquidity buffers to counter or ride out any future recession. The current monetary policy of low short-term and long-term interest rates constrains the ability of banks to generate net interest income. Plus, since credit remains the main income source for most Euro area banks, business models clearly need to adapt to the realities of this new financial environment if banks are to generate sustainable profit. While it’s true that many EU banks have announced financial margin improvement in recent years, analysts believe this results from more efficient operations rather than implementing in-depth adaptive structural challenges.

Following the financial crisis, fees and commissions have become an increasingly important income source for Euro area banks. According to ECB data, the close of 2015 saw the average fees and commission income of banks in the Euro area representing almost 30% of total operating income. Deeper analysis of this income shows that fees resulting from the operation of payment services represented the largest single category (18%), followed by asset management (15%), distributed investment products (13%) and securities (10%). Given these figures, it’s understandable that the release of the PSD2, which creates pressure in the payments market from new TPP competitors, and requires investment in APIs and new authentication technologies, has not been warmly welcomed by the banks – many of which view it as a further barrier that will hamper their return to robust profitability.

Yet the PSD2 also represents a new business opportunity for the banking industry - one that drives the uptake of IT technology (artificial intelligence algorithms, expert systems, new channels to advertise and communicate with customers, cloud-based banking) that will ultimately help to consolidate the position of banks in the core of the retail payments market. Despite varying levels of enthusiasm about embracing Open Banking, commercial banks are toeing the line – primarily for mandatory compliance, rather than business reasons. That said, some tech savvy banks are seizing the PSD2 opportunity and undertaking a major reorganization of the way they offer banking services to their customers. Indeed, some credit institutions now advertise themselves as being a *bank-as-a set-of API-accessed services* – an approach that will substantially change the way banks are perceived.

While Open Banking will most likely become just one more step in the ongoing digital transformation of banking, it’s a step forward that has potentially significant market structure consequences. Banks and TPPs will compete for the provision of some financial services. But financial regulators also want to see stronger collaboration between payment market incumbents and incomers. Payment Service Providers are responsible for the compliance of payment solutions with the regulations, but all stakeholders within the payments industry will be impacted by the PSD2 and the RTS on SCA. Finally, TPPs will compete between themselves and with banks for the capture of a substantial part of this new market.

Open Banking represents a very substantial change in the way financial services are operated and delivered – one in which financial data will be shared, processed and monetized. The technology deployed to update core payment processing systems may have a substantial impact on structuring the offer side of the Open Banking market.

2. The Disruptive Potential of the Technology Applied to Open Banking

Payment Account Aggregation Related Services (AIPSP)

Banks need to recoup the significant investment required to transform their outdated legacy platforms and infrastructures by finding ways to monetize TPP access to their customer payment account data – and this may involve working together to establish new business models around APIs. Many national banks have already successfully cooperated to develop common API specifications, while different banking associations have adopted a highly consensual approach when negotiating the practicalities of deploying PSD2 APIs. This consensus extends to establishing common positions on (1) the nature of the payment account information to be accessed by TPPs (2) the conditions for API access by TPPs, and (3) authentication and proof of consent by the bank's customer. Clearly, the challenging changes being driven by Open Banking have pushed banks to enhance their collaboration.

TPP account aggregation services will generate a huge amount of customer data for delivery to the TPPs; information flows that will be used to provide tailored financial services (such as insurance or investment strategy). Artificial intelligence (AI) software will help to identify generic patterns of customer expending behavior from rough data, as well as categories of individual financial profiles. If the possession of good quality customer data is the new target for competition, then those organizations sharing data (banks or incomers) will gain a clear competitive advantage. Customer data will become a financial asset and, as such, could be monetized. Because access to customer data by a TPP is a legal requirement, that's a free service. However, upon customer consent, access to bank account information beyond what the PSD2 strictly requires could be billed (for example, providing access to deposit or saving accounts).

However, AI machine learning algorithms are only as good as the quality of the data used to train them. More good quality data means faster algorithmic machine learning and a shorter time-to-market for new financial products. Thus, AI algorithms offer an opportunity for both banks and their competitors to enable differentiated financial services. TPP aggregators are a good case for AI: big data has to be processed in real-time – and that requires both computing power and optimized algorithms. For smaller banks or FinTechs, access to such resources are not assured, while medium-sized banks will struggle to invest in AI technology and remain competitive.

Business models based on big data favor those rich in data. As the World Bank recently pointed out, deployment of AI technology driven by the need to monetize data aggregation may favor greater concentration of the retail banking market. Thus, AI will allow new financial offerings to be built and scaled much more efficiently. In this context, PSD2 can favor the elimination of mid-sized banks struggling to remain competitive - either by merging to reach a critical mass, or by focusing on niche markets and competing directly with FinTech financial services firms. A comparable effect has taken place in past years in the card payments market, which is also under the scope of the PSD2. The recent Eurosystem Report, Card Payments in Europe, highlights how international card schemes have taken a greater share of the market compared to domestic schemes in the EEA. One of the reasons for this growth was identified as the impact of the Interchange Fee Regulation.

Finally, the boost in the number of financial services offered - brought about by PSD2 market dynamics - might speed up commoditization and facilitate the capture of customers from smaller banks. Big banks have a natural cost advantage that will support their capture of customers from mid-sized players, especially if there's an overall bank revenue fall as a result of successful competition by TPPs. Overall, compliance with the PSD2 and the need to invest in costly IT technology may incentivize banking market concentration – particularly in the medium-sized segment. Smaller actors may merge to manage platforms of financial services accessed through APIs boosted by AI-enabled data analytics and establish new models for relationships with existing and future customers.

It remains that the dynamics of the banking market are slow and new business models will take time – potentially decades - to consolidate. Moreover, individual banks or bank associations may also play a TPP role, competing or reaching agreements with *pure* FinTech TPPs who have the technology required to serve niche financial products and services and/or specific customer segments. The SPA opinion is that PSD2 will not relegate the banks to mere payment account holders and funds transfer operators.

TPPs Offering Payment Initiation Services (PISP)

PISPs are a use case for (instant) credit transfers. On agreement between the retailer and the consumer, the PISP will initiate the payment using a designated bank payment account through the bank's API. Once authorized, the payment itself will be exclusively executed in the inter-bank domain because the PSD2 sets out that the PISP cannot hold customer funds at any time. It follows that PISP will not create any systemic risk. However, the TPP-PISP plays an additional intermediary role in the payment processing chain and, as such, adds its own vulnerabilities. Some of these are addressed by the Regulatory Technical Standards (RTS) for strong customer authentication and common and secure open standards of communication that mandate, for example, the PISP must be identified by the customer bank (ASPSP) using an e-IDAS certificate. However, SPA considers that a complete security model for the TPP-centric technical architecture is needed. The ISO TC68 has started work on this area and SPA members are involved in this project.

The impact assessment of TPP-PISP services on the Open Banking ecosystem varies, depending on the role of each key player:

- Retailers

Payment account access services meet the retailer requirements of being able to offer an (instant) credit transfer as a payment method at check out. SEPA instant credit transfers offered by the PISP will be therefore in direct competition with the card, especially for e-commerce payments. Merchants accepting PISP payments will in theory benefit from this competition effect between SEPA payment instruments. Other than the security aspects highlighted previously, the use of PISP services may result in a lack of convenience for consumers that leads them to abandon purchases. Since the PISP plays an extra role in the payment chain, there will be additional communication/sessions and redirections required to comply with the legal customer authentication requirements.

The PSD2 establishes that customer authentication is usually the responsibility of the bank designated by the consumer. This means that the PISP must generate an authentication request through the bank API as part of the payment initiation process. In other words, how the bank proceeds with the transaction is not within the control of the PISP or the retailer. For example, the bank may decide to apply an exemption to the Strong Customer Authentication if its real-time risk transaction analysis categorizes a specific payment as low risk.

In this respect, both the TPP-PISP and the retailer must rely on the efficiency of the authentication methods and the reliability of the API offered by the designated banks. Because not all bank APIs offer the same services, and banks may choose different authentication solutions, there is an uncertainty about the final quality of the service offered by the TPP-PISP to both retailers and consumers. This lack of harmonization may hamper the development of the PISP market.

SPA believes that a standard framework for PISP services, streamlining the payment flow and granting the retailer freedom of choice of its PISP, should be beneficial for the retail sector. Section 5 of this document provides further details of the SPA standardization initiatives in this area.

▸ Banks

Banks must (1) issue personal security credentials (PSC) that a customer can use to initiate a payment using TPP services and (2) offer and maintain an open API that enables the TPP-PISP to initiate a payment, typically using the IBAN of the customer. In the TPP-PISP context, the customer's bank has two main legal obligations: to strongly authenticate the customer and to execute the payment.

The execution of an instant payment initiated by a PISP is a legal requirement that the bank should in principle provide for free. TPP services are provided through an API that banks could monetize. The mandatory dedicated interface for PISPs could become the core of a more extended API that provides small and medium sized enterprises (SMEs) with access to instant payments services, or become one of a portfolio of services (that could include cash and liquidity risk management) to compete with banks.

▸ Customers

PSD2 empowers bank customers to grant consent to a third party TPPs for access to their payment bank account information. The real value for the customer is more apparent when the two roles (PISP + AISP) are played by the TPP, which becomes able to offer value-added services before initiating an instant payment. If the TPP limits activity to payment initiation, it is SPA's opinion that there is no obvious benefit for the consumer to choose a PISP to pay instead of using a card. As a result, the consumer will need to be incentivized to use this method – either by through loyalty services provided by the retailer or through some form of free account information services from the TPP-PISP.

Based on the above considerations, SPA does not believe that PISP activity will have a strong impact in the EEA retail payments market structure in the short term. Rather, the PSD2 is likely to create competition between existing PISP players and market incomers.

It remains true that the potential for market evolution will depend on the ability of TPPs to offer attractive, personalized financial services using customer account data they collect acting as an AISP. For PISPs, SPA believes that the following five factors will be conditional on business success:

1. The implementation models that will prevail – either proprietary solutions by individual TPP-PISPs or federations of existing initiatives benefiting from volume effects
2. The extent to which banks will decide to play the TPP role directly by themselves
3. The ability of the deployed technical solutions to reduce customer friction during the authentication process
4. The ability to achieve a low level of fraud by enabling a significant volume of transactions to fall under an exemption regime for strong customer authentication
5. The success of the competing EMVCo Secure Remote Commerce Framework.

3. Open Banking Customer Authentication and Consent Under PSD2

Strong Customer Authentication and Consent

Strong Customer Authentication (SCA) is clearly defined by the PSD2 and the RTS on SCA provides some high-level implementation details and describes the conditions under which certain payment transactions might be exempted from SCA. It should be noted that the RTS on SCA requires the generation of an authentication code as a result of the validation of at least two authentication elements of different categories (something you know, something you have, an inherent feature) and independent from the security point of view. When the transaction is online, the authentication code must be generated in a specific way – known as dynamic linking.

Dynamic linking refers to the generation of an authentication code with specific security properties for the SCA of online payments which don't fall under the exemption regime. The authentication code generated has to include both the amount to be paid and the identity of the payee in a way that proves consent by the payer for this payment, and dynamic linking ensures that the authentication code cannot be replayed.

In practice, the authentication code with dynamic linking will be implemented as a cryptogram. At least six elements should be included in the calculation of the cryptogram: the proof of the successful authentication using the two independent authentication elements, the amount, the payee, the consent by the payer, and a unique identifier for the transaction. The consent by the payer may be considered as granted if the authentication takes place after the customer is aware of the amount and of the payee. **In that case, the willingness of the payer to be authenticated is equivalent to a consent for the payment to proceed**.

Consent can only be considered as valid if the customer payment device ensures the information displayed to the payer (amount, payee) is the data effectively used to calculate the cryptogram validating the payment order. Therefore, the intrinsic value of the cryptogram as providing payer consent evidence relies on the level of security provided by the authentication elements used to generate the cryptogram. Section 4 of this paper provides a fuller discussion on the level of security provided by different authentication technologies.

A Flexible Framework Customer Authentication in an Open Banking Context

Other than security, the use of frictionless authentication methods is a key concern for retailers. This is particularly true for e-commerce payments intermediated by a TPP, which could involve successive redirections of the consumer's interface and the risk of a poorly perceived experience.

Retailers want more flexible payment solutions that protect them against fraud and are adapted to address growing consumer demand for payment convenience. The ability for retailers to establish (and protect) a consumer's identity early on in the transaction (for example, after connecting to a retailer site) is a prime differentiator that may result in better shopping experience that becomes a key loyalty factor.

The PSD2 approach to verifying a consumer's digital identity is through SCA. Ideally, SCA solutions should enable banks and retailers to verify any consumer identity across all their payment channels. If a consumer can be identified by the retailer, the retailer is in a very good position to assess the customer's risk profile and propose an exemption to SCA. The retailer assessment could be part of the information used by a TPP to initiate a SCA-not-required payment. Yet the EBA's Opinion, released in June 2018, is formal on this point: only banks may decide an exemption to the SCA for a credit transfer - even the TPP cannot apply for an exemption.

This creates a challenge: how to associate retailers to the SCA process when a payment is initiated by a TPP that is contracted with a retailer (TPP/Retailer peer). The issue could be reformulated as: (1) to what extent a TPP can rely on the authentication elements that banks issue to their customers for SCA purposes, and (2) if some kind of contractual delegation to the TPP/Retailer peer for SCA is a realistic option. The EBA's Opinion of June 18 is clear on this point: the bank may contractually delegate the SCA on a TPP. This contract should fix the requirements to manage the personalized security credentials of the customer and allocate liability in the event of repudiation, technical problems, security incidents, misuse of personal data or fraud.

One problem with SCA delegation is that it relies on a bilateral contractual agreement between a TPP and a bank. The TPP needs to individually sign a contract for SCA delegation with many banks to address all its customers. This will not scale unless there is a framework agreement in place that federates banks and TPPs.

SPA believes that these two issues - customer redirection as the authentication method for SCA in an Open Banking context and the generalization of the SCA delegation being unrealistic in the short term – means that there is also room for two other authentication methods: embedded and out-of-the-band. We note that the Berlin Group API already supports these three authentication methods: redirection, out-of-the-band and embedded. Some argue that the answer should be a new standard API infrastructure that could deal with all authentication methods seamlessly, leaving the choice to the TPP based on the available personal security credentials of an individual customer. But while this is an attractive proposition, it's not without its own complexities - both legal and technical.

In embedded mode, the customer never leaves the TPP interface during the authentication process, which is performed by the bank using authentication credentials under the bank's responsibility. The embedded authentication is a compromise: the consumer experience is preserved because the same user interface is presented to the user throughout the transaction and friction (due to redirections) is avoided. Because the SCA itself is carried out by the bank, the API must support the transmission of the data elements required for authentication. Implementation of the embedded method may require Personalized Security Credentials issued by the bank to be personalized in a consumer device – for instance, in a mobile wallet issued by a third party. SPA notes that this scenario was mentioned in the EBA Opinion of June 2018.

In other implementations, the user enters the bank-generated password and OTP into the TPP interface. These credentials are then transmitted by the TPP to the bank for verification. SPA points out that this method is akin to phishing attacks, and a user may not be able to distinguish a genuine TPP from a hacker. Therefore, SPA is of the opinion that the embedded model is better implemented with security credentials issued by the bank, personalized in the user device, as in the Apple Pay solution. SPA also notes that FIDO authentication may be used in this implementation.

The SPA opinion is that any future technical European standard should provide flexibility when it comes to choosing the most appropriate authentication method to ease the consumer payment experience. SPA considers that in a future process of convergence between existing API specifications, the common functional criteria should include support for four authentication methods: redirect, decoupled, embedded and delegated. Additional discussion elements on the feasibility of a common European standard can be found in Section 5 of this paper.

4. Including Card Technology in the Open Banking Ecosystem

Biometrics and card technology match for strong customer authentication

Both the PSD2 and the RTS on Strong Customer Authentication are legal texts and in principle are technologically neutral. The RTS on SCA, however, does provide some technical details: eligible authentication elements must belong to one of the three classical categories: knowledge, possession and inherence, and must be independent from a security point of view. The RTS on SCA also lays down security requirements that ensure protection of the authentication elements against unauthorized use or disclosure.

SPA points out, however, that the effective isolation of the authentication elements - their integrity and confidentiality - is highly dependent on the security of the underlying technology. This is particularly true when biometrics are used as one of the two authentication elements. Biometric data has been identified as sensitive personal data and its processing is subject to specific requirements according to the General Data Protection Regulation (GDPR). Biometrics have many advantages as an authentication factor, provided that the certified biometrics reference is securely stored in a device under the exclusive control of the customer.

Smart card technology is tailored for biometrics storage and matching, ensuring that once personalized the biometrics never leaves the card. In this way, security for the authentication process and privacy are both guaranteed. Years ago, SPA pioneered the use of biometrics for card payments and encouraged EMVCo to develop EMV biometric specifications. Today, of EMVCo members are making efforts to leverage the use of biometrics in their respective specifications.

Card technology to initiate an Instant Payment

Cards can be used to secure retail payments in a variety of different scenarios:

1. As a general payment instrument issued by the bank that holds the payment account associated with the card. These are usually issued as debit or credit plastic cards.
2. As a payment instrument issued by a retailer, whose acceptance is restricted to this retailer or to other acceptors having a contractual agreement with the issuer-retailer. Often these cards are associated to revolving credit and are expensive for the consumer.
3. As a two-factor authenticator to initiate a non-card payment (for example, an instant payment).

Use cases 1 and 2 listed above both correspond to the usual way in which a card is used, but it is use case 3 that is the most interesting in the context of Open Banking. SPA is investigating this use case as an enabler for instant payments and considers that two scenarios could in principle be differentiated:

1. An authentication application could be added to a bank-issued payment card (use case 1) and used in a POI which supports both card and instant payments.
2. A card issued by a TPP/retailer and personalized with a proxy of the IBAN of the consumer bank account. The card could be used to pay at a POI or online.

Both approaches have pros and cons. SPA considers that different contractual agreements would be required for the implementation and certification of these cards. SPA is currently in talks with other payments stakeholders to better understand how the card could better fit into their business development plans and our conclusions will be addressed in a future paper.

5. SPA Standardization Efforts for TPP-Initiated Services

Why Technical Standardization for Compliance with PSD2 is Difficult

One common argument against the PSD2 and the RTS on SCA is the aggressive deadline for conformance. Moreover, the PSD2 does not mandate that a single standard dedicated interface is to be implemented by banks. Both the factors have served to discourage the development of a pan-European standard for harmonized API implementations of the PSD2.

Instead, several national banking common API initiatives have been initiated. Examples include the Open Banking API in UK, the STET API in France, and the Berlin Group Specifications (which have a broader audience). Yet these initiatives also contribute to market fragmentation, an undesirable side-effect from the regulator's perspective. It's certain that harmonization of these APIs could facilitate access by TPPs operating at a European scale and help to develop the Open Banking market.

Another issue is the scope of this standardization effort. SPA believes that beyond the API (messages to be exchanged between the TPP and the ASPSP), a complete Open Banking framework for interoperability should be standardized. This might include the data flows for the different stages at check-out in the retailer domain and conclude with the notification to the retailer that the funds from the consumer's account have been effectively transferred. Catalyzed by different SEPA representative instances (for example, the European Retail Payments Board) partial initiatives in that direction have recently been launched (such as the European Payment Council's Request to Pay). Another relevant initiative to establish an Open Banking standardization framework is ongoing (the European Payment Council's Multi-Stakeholder Group on Mobile SEPA Credit Transfers). SPA considers that prior to the revision of the PSD2, it would be interesting to evaluate the overall picture.

From a security viewpoint, a security architecture with standard mechanisms based on robust ISO cryptographic mechanisms could be valuable to mitigate vulnerabilities – those that result from the central switch role played by the TPP. The TPP develops and maintains interfaces over open networks with retailers, banks (through the API), consumers and possibly other entities (such as certification authorities and ID management systems). The compromise of TPP data might in theory have significant consequences that need to be better understood and addressed before initiating any standardization effort.

Finally, the standardization of security mechanisms for Open Banking must be supported by a Certification Framework for Open Banking processing devices. That's a complex and long program to implement. In any respect, SPA's opinion is that the future update of the European Regulatory Framework (the PSD3) will see the legal texts become more prescriptive in terms of standardization.

The Role of SPA in the Standardization of Open Banking

SPA is a major contributor to the standardization efforts of the payment industry, both at a European and international level. SPA does not attempt to prescribe specific security or technical Open Banking authentication solutions; its role is to promote the adoption of trusted payment technology by the industry. We believe that the integration of card technology for authentication and payment into TPP-intermediated transactions will bring benefits to the Open Banking ecosystem.

Because Open Banking is a global trend, ISO TC68 has taken the lead for the partial standardization of the ecosystem. SPA members are involved in different ISO TC68 standardization initiatives on two projects:

- An ISO Technical Specification that is being created under the responsibility of ISO TC68 SC9. This initiative was inspired by the UK Open Banking specification that proposed a common approach for the development of Open APIs rather than a single standard API.
- An ISO standard (ISO 23195) setting out the Security Objectives for TPP-initiated financial services under the responsibility of ISO TC68 SC2 WG16. This initial standard should be completed with a second one more focused on the Security Architecture aspects for Open Banking.

SPA is also active in SEPA initiatives to develop a standardization framework for SEPA Mobile Credit Transfers. Because (instant) SEPA credit transfers is the payment instrument used by the industry for TPP Payments, the outcome of this effort will help to build and sustain the SEPA Open Banking Standardization Framework.

SPA Concluding Observations

1. PSD2 introduces a real revolution (Open Banking) in the way financial services may be offered to the bank customer by opening, in a secure way, access to the bank payment account by a third party. All participants in the Open Banking ecosystem, and especially banks, must update their processing infrastructures and build new interfaces to comply with the PSD2
2. The PSD2 empowers bank customers with the right to grant access to designated third parties (regulated TPPs) to information about movements on the payment accounts they hold with banks. Banks must provide the TPP with interfaces featuring a sufficient level of performance and security. Otherwise they cannot benefit of an exemption to provide a fallback solution to the TPP
3. Because of Points 1 and 2 above, SPA believes that the new Open Banking ecosystem is disruptive. TPPs could in theory relegate banks to the role of payment processors and account holding providers, or at the very least become serious competitors to banks for certain financial services
4. However, SPA believes that banks will continue to play a central role in the retail payments market, not merely as payment account servicing providers, but as the main issuers of payment and authentication personal credentials used for the provision of their own banking financial services.
5. The Open Banking ecosystem brings additional vulnerabilities to payment systems and subsequent threats to the integrity of customer funds held in bank payment accounts. SPA believes that Strong Customer Authentication is the proper countermeasure to address these risks, provided that the pan-European harmonization of solutions is ensured.
6. SPA prompts people to remember that not all authentication elements, even those that apply to categories of the PSD2 and the RTS on SCA, are equivalent from a security point of view. SPA considers that card technology combined with biometrics is a very secure and convenient method to conform to the new regulatory framework.
7. Speed and convenience at the check-out are key concerns for consumers when purchasing online. Online retailers constantly reiterate how the lack of tolerance for checkout friction among online consumers frequently results in cart abandonments. The problem here is that using TPP payment services at check-out will lead to more friction.
8. Authentication methods appropriate to the TPP context should be privileged. SPA believes that an Open Standard API should enable any of the four authentication methods described in this document: customer redirection, embedded, decoupled and delegated customer authentication.
9. SPA members are actively participating in European and global standardization efforts to ensure that Open Banking standards, and their authentication methods, provide a flexible and fully secured ecosystem that preserves the interests of all the stakeholders.