



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ

Master Thesis

*Analysis and overview of security measures for
banking transactions under EU PSD/2*



University of the Aegean
Department of Information and Communication Systems
Engineering (ICSD)

MASTER THESIS

*Submitted in partial fulfillment of the requirements for the
degree of Master “Information and Communication Systems Security”*

***“Analysis and overview of security measures for banking
transactions under EU PSD/2”***

by
Marianna Gounari

Supervisor: Georgios Stergiopoulos
Committee: Lilian Mitrou, Maria Karyda
Student Number: 3232020007

Academic year 2022-23

Working with this thesis has been a demanding process, but also a rewarding and exciting experience in terms of learning and developing my analytical and research skills.

To that end, I would like to express my sincere gratitude to my supervisor Stergiopoulos Georgios for his provision of expertise and insights into the subject and his time spent, and also for his guidance and constructive feedback throughout the writing process. It would not have been possible to perform this thesis without the help and support received along the way.

Moreover, I would like to thank the University of the Aegean that offered me the opportunity to scientifically specialize my knowledge in the field of Information and Communication Systems Security through the solid, integrated and high scientific postgraduate program it provided me as a student.

Last but not least, I wish to dedicate this achievement to all my family, who with love and effort accompanied me in this process, without hesitating at any moment of seeing my dreams come true, which are also their dreams. A special feeling of gratitude to my mother and grandmother, whose strength is always a driving force for me to try and achieve every goal I set in life.

Marianna, May 2023

Analysis and overview of security measures for banking transactions under EU PSD/2

Marianna Gounari

“Information and Communication Systems Security” Master Programme, 2022-2023

Department of Information and Communication Systems Engineering (ICSD),
University of the Aegean

Abstract

This thesis focuses on the security measures implemented in banking transactions within the European Economic Area (EEA) in accordance with the Second or Revised Payment Service Directive (PSD2 or Directive hereafter). PSD2 is a policy intended to make the European payments system more connected and efficient, making payments easier and more secure and encourage innovation and competition in the industry. As far as the primary challenge for banks is that PSD2 requires them to grant third parties' access to their customer data via open Application Programming Interfaces (APIs), the likelihood of potential risks and threats emerging in the customers' payment data exchanged, and thus the various payment transactions performed, is now higher. Consequently, the Directive has included, in addition to the essential rights and obligations that all stakeholders must follow, a number of specific security measures and standards that banks and relevant parties must adopt. As a result, the primary goal of this thesis is to investigate and analyze these security measures for banking transactions under EU PSD2 in order to provide better guidance and understanding to traditional banks and stakeholders during implementation, as well as their impact in terms of protecting transactions, data, and payment services. The thesis mainly draws on the doctrinal research method, which is a “typical legal research” method that considers laws, regulations, guidelines, standards, and cases, as well as other legal sources (e.g., PSD2, PCI DSS, ISO/IEC 27000 series, GDPR, EBA, EDPB Guidelines). It is also based on literature evaluations and secondary sources (e.g., books and articles). We concluded from an extensive review of PSD2 security requirements and measures that there is a lack of harmonization and clarity identified almost by all MS, which justifies the fact that it becomes difficult for banks to comprehend the entire range of PSD2 compliance obligations. Although the completion of the EBA RTS was an important milestone that provided firms with greater clarity and certainty on how to move forward with their PSD2 compliance and strategic programs, it still leaves a number of important questions for stakeholders regarding the technical security specifications (e.g., APIs, dedicated or user-facing interfaces) on which they should rely and implement in the context

of PSD2 compliance. Even when the EBA's RTS is released, it is unknown what the authentication technology (SCA) will finally look like. Furthermore, the PSPs' flexibility to establish authentication as they see fit trumps the interest in making this procedure as secure as possible. The compromise on the legality of screen scraping results in a similar conclusion. Because Third-Party Provider (TPP) services rely on the use of sensitive personal and financial data, it opens up the market to a greater number of competitors while also relying heavily on the IT infrastructure of several parties, a number of risks have been identified [85]. In general, the introduction of TPP into the market made present online PSPs a target for hackers, as a considerable number of frauds emerged in tandem with the expansion in e-commerce transactions. Furthermore, users' personal data are not effectively protected because various issues exist between the GDPR and PSD2. While PSD2 poses serious threats to current business models, banks may be able to adapt them in a technologically innovative way by implementing specific practices and business models, strategies, and more proper API management. Last but not least, the EU should specify how existing standards organizations should interact with the PSD2 specifications developed by the European Payments Council. The interaction between PSD2, ISO/IEC 27001:2022, and PCI DSS analyzed at the end of the thesis indirectly demonstrates this requirement [73].

Table of Contents

Definitions.....	8
Introduction.....	11
Background and Problem Statement.....	11
Purpose.....	12
Literature Review	13
Structure	13
Section 1 - PSD2: A General Overview	13
Objective	13
Introduction	13
Consumers rights	15
Payment Security	17
Third-Party Access.....	17
Implementation Scope.....	17
Payment Services	17
Stakeholders	19
Geographical scope	23
Section 2 – Rights and Obligations.....	25
Introduction.....	25
Authorization and Registration of PIs	26
Application.....	26
NCA Public Register	30
Home and Host Member State Cooperation.....	32
EBA Register.....	35
Access to Payments Systems.....	37
Access to accounts maintained with a credit institution	38
Provision and Use of Payment Services	38
Authorization of Payment Transactions.....	39
Execution of Payment Transactions	46
Information and Conditions	50
Single Payment Transactions	51
Framework contract.....	51
Currency	53
Charges.....	53
Dispute Resolution.....	55
Section 3 - Security Measures	55
Introduction.....	55
Common and Secure Open Standards of Communication (CSC)	57

Open Banking API Standardization	58
TTP User Management.....	61
Secure Communication Session.....	67
Data Exchanges	67
Strong Customer Authentication (SCA).....	69
Transaction Monitoring	72
Security Measures Review	72
One-Time Authentication Code.....	73
Dynamic Linking	75
SCA Elements Requirements	76
SCA Interface Implementation	79
SCA Exemptions.....	82
Personalized Security Credentials (PSC) Protection	86
Security and Operational Risk Management.....	88
Governance	89
Risk Assessment	90
Protection	91
Detection.....	96
Business Continuity Management.....	99
Testing of Security Measures	101
Situational Awareness and Continuous Learning	102
Payment Service User Relationship Management	102
Mapping Table: PSD2 – ISO/IEC 27001:2022 – PCI DSS	103
Discussion and Conclusions.....	112
References.....	117

Definitions

For the purposes of this thesis, the following definitions apply:

- (1) The term 'home Member State' refers to either the Member State in which the PSP's registered office is located, or, if the PSP has no registered office under its national law, the Member State in which its head office is located.
- (2) The term "host Member State" refers to a Member State other than the home Member State in which a PSP has an agent, a branch, or provides payment services.
- (3) The term "payment service" refers to any of the business activities listed in Annex I.
- (4) A 'PI' is a legal person who has been authorized by Article 11 to provide and execute payment services throughout the Union.
- (5) A 'payment transaction' is an act of placing, transferring, or withdrawing funds initiated by the payer or on his behalf or by the payee, regardless of any underlying obligations between the payer and the payee.
- (6) A 'remote payment transaction' is one that is initiated over the internet or through a device capable of long-distance communication.
- (7) The term "payment system" refers to a funds transfer system that has formal and standardized arrangements and common rules for the processing, clearing, and/or settlement of payment transactions.
- (8) A 'payer' is a natural or legal person who holds a payment account and allows a payment order from that payment account, or a natural or legal person who gives a payment order in the absence of a payment account.
- (9) A 'payee' is a natural or legal person who is the intended recipient of funds that have been the subject of a payment transaction;
- (10) A 'payment service user' is a natural or legal person who uses a payment service as a payer, payee, or both.
- (11) A 'PSP' is a body referred to in Article 1(1) or a natural or legal person who is exempt under Article 32 or 33.
- (12) 'payment account' refers to an account held in the name of one or more payment service users and used for the execution of payment transactions; (13) 'payment order' refers to an instruction issued by a payer or payee to its PSP requesting the execution of a payment transaction.
- (14) A personalized device(s) and/or set of procedures agreed between the payment service user and the PSP and used to initiate a payment order are referred to as a 'payment instrument.'
- (15) A 'payment initiation service' is a service that initiates a payment order at the payment service user's request in relation to a payment account held by another PSP.
- (16) 'account information service' refers to an online service that provides consolidated information on one or more payment accounts held by the payment service user with another PSP or more than one PSP.

(17) 'account servicing PSP' refers to a PSP that provides and maintains a payment account for a payer.

(18) 'payment initiation service provider' means a PSP engaged in business activities as defined in Annex I point (7).

(19) 'account information service provider' means a PSP engaged in business activities as defined in Annex I point (8).

(20) 'consumer' means a natural person acting for purposes other than his or her trade, business, or profession in payment service contracts covered by this Directive.

(21) 'framework contract' means a payment service contract that governs the future execution of individual and successive payment transactions and may contain the obligation and conditions for opening a payment account.

(22) A 'money remittance' payment service is one in which funds are received from a payer without any payment accounts being established in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or another PSP acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

(23) The term “direct debit” refers to a payment service for debiting a payer's payment account in which a payment transaction is initiated by the payee based on the payer's consent given to the payee, the payee's PSP, or the payer's own PSP.

(24) A 'credit transfer' is a payment service in which a payment transaction or a series of payment transactions are credited to a payee's payment account from a payer's payment account by the PSP that holds the payer's payment account, based on an instruction given by the payer.

(25) 'Funds' means banknotes and coins, scriptural money, or electronic money, as defined in Article 2(2) of Directive 2009/110/EC.

(26) A 'value date' is a time reference used by a PSP to calculate interest on funds debited or credited to a payment account.

(27) 'reference exchange rate' means the exchange rate used as the basis for calculating any currency exchange and is made available by the PSP or comes from a publicly available source that can be verified by both parties to a payment service contract.

(28) 'reference interest rate' means the interest rate used as the basis for calculating any interest to be applied and comes from a publicly available source that can be verified by both parties to a payment service contract.

(29) The term “authentication” refers to a procedure that allows a PSP to verify a payment service user's identity or the validity of the use of a specific payment instrument, including the use of the user's personalized security credentials.

(30) 'Strong customer authentication' refers to authentication based on the use of two or more elements classified as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is) that are independent, in the sense that a breach of one does not compromise the reliability of the others, and is designed to protect the confidentiality of the authentication data.

(31) “personalized security credentials” refers to personalized features provided by a PSP to a payment service user for authentication purposes.

(32) “sensitive payment data” refers to information, including personalized security credentials, that can be used to commit fraud. The name of the account owner and the account number do not constitute sensitive payment data for the activities of payment initiation service providers and account information service providers.

(33) A 'unique identifier' is a combination of letters, numbers, or symbols specified by the PSP and provided by the payment service user to identify unambiguously another payment service user and/or that other payment service user's payment account for a payment transaction.

(34) 'means of distance communication' means any method that allows the PSP and the payment service user to conclude a payment services contract without their simultaneous physical presence.

(35) 'durable medium' means any instrument that allows the payment service user to store information addressed personally to that payment service user in a way that is accessible for future reference for a period of time adequate to the purposes of the contract.

(36) A 'microenterprise' is defined as an enterprise at the time of the payment service contract as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC.

(37) 'business day' means a day on which the relevant PSP of the payer or the PSP of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction.

(38) 'agent' means a natural or legal person who acts on behalf of a PI in providing payment services.

(39) A 'branch' is a place of business other than the head office that is a part of a PI, has no legal personality, and carries out directly some or all of the transactions inherent in a PI's business; all of the places of business established in the same Member State by a PI with a head office in another Member State shall be treated as a single branch.

(40) 'group' means a collection of undertakings linked by a relationship referred to in Article 22(1), (2), or (7) of Directive 2013/34/EU, or undertakings as defined in Articles 4, 5, 6, and 7 of Commission Delegated Regulation (EU) No 241/2014 (2), linked by a relationship referred to in Article 10(1) or Article 113(6) or (7) of Regulation (EU) No 575/2013.

(41) 'electronic communications network' means a network as defined in Article 2 point (a) of Directive 2002/21/EC of the European Parliament and of the Council (3).

(42) 'electronic communications service' means a service as defined in Article 2 point (c) of Directive 2002/21/EC.

(43) 'Digital content' refers to goods or services produced and supplied in digital form, the use or consumption of which is limited to a technical device and does not include the use or consumption of physical goods or services in any way.

(44) A payment service provided by a PSP contracting with a payee to accept and process payment transactions, resulting in a transfer of funds to the payee is referred to as 'acquiring of payment transactions'.

(45) A payment service by a PSP contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions is referred to as “issuing of payment instruments”.

(46) 'Own funds' means funds as defined in point 118 of Article 4(1) of Regulation (EU) No 575/2013, where at least 75% of Tier 1 capital is Common Equity Tier 1 capital as defined in Article 50 of that Regulation and Tier 2 is equal to or less than one-third of Tier 1 capital;

(47) A 'payment brand' is any material or digital name, term, sign, symbol, or combination of them capable of indicating which payment card scheme card-based payment transactions are conducted under.

(48) The inclusion of two or more payment brands or payment applications from the same payment brand on the same payment instrument is referred to as co-badging [25] [26] [10].

Introduction

Background and Problem Statement

Over the last few decades, technology has brought about incredible changes in many aspects of daily life. The widespread use of the telephone, radio, television, mobile phone, internet, and other latest digital technologies, particularly in payment services, has disrupted the current status quo, created new realities, and forced incumbent and potential new players to adopt the latest developments. As a result of the latest technological developments in the payment sector and the increase in e-commerce, PSPs must provide their services faster, better, and more user-friendly, as well as provide their users with more options for selecting the best fit services for their needs. As a result of these developments, many users, particularly millennials, prefer to make payments seamlessly via their mobile phones and wearables (e.g., the AppleWatch, Samsung's Gear smartwatches) without wasting time or effort. Because PSPs must access their users' relevant personal data and information in order to provide a more user-friendly payment experience, payment transaction security and data privacy are critical issues for the payment sector. As a result, the EU and some other countries (for example, Singapore and the United States) took steps to regulate such developments in the online/mobile payment sector.

Following such trend in the payment sector, due to the emergence of the data-driven technologies, the Second/ Revised Payment Service Directive (PSD2 or Directive hereafter), a European Union (EU) legislative instrument, was adopted on 8 October 2015 to catch up with digital and technological changes in online payment transactions. Prior to PSD2, the (first) Payment Service Directive (PSD1) went into effect on December 25, 2007, to create an EU-wide internal market for all types of electronic and non-cash payments (e.g., card payments, mobile and online payments, direct debits, and credit transfers).

PSD2 was created to address new technological developments and to replace PSD1. Then, to supply their services, new and unconventional actors were included in the internet payment services regulatory framework. PSD2 added two new service types: Account Information Services (AIS) and Payment Initiation Services (PIS). Payment Initiation

Service Providers (PISPs) (e.g., PayPal, Sofort, iDeal, Tikkie) initiate payment orders from the user's bank account following the user's request; Account Information Service Providers (AISPs) (e.g., Moneybox, Spiir, Trustly, Fintonic) display consolidated information obtained from the user's one or more bank accounts. Although PISPs and AISPs existed prior to PSD2, the main change brought about by PSD2 is the regulation of PISPs and AISPs and the establishment of the legal ground for their operation in the online payment market. To provide their innovative services, these Third-Party Providers (TPPs), which include both PISPs and AISPs, must gain access to the relevant payment account information and personal data of the users [88].

It is true that the introduction of PSD2 into the payment sector provided numerous benefits in terms of information security and data protection. However, practically all Member States (MSs) have observed a lack of consistency and clarity in terms of security standards and measures defined at the same time. This explains why banks (or else Account Servicing Payment Services Providers (ASPSPs)) find it difficult to understand the full scope of their compliance obligations. Although the finalization of the European Banking Authority's (EBA) Regulatory Technical Standards (RTS) was an important milestone that provided firms with greater clarity and certainty on how to move forward with their PSD2 compliance and strategic programs, it still leaves a number of important questions for stakeholders regarding the technical specifications they should rely on and implement in the context of the PSD2 compliance. Therefore, an analysis and study of the security measures covered by PSD2 are deemed critical in order for stakeholders to be properly compliant with the Directive.

Purpose

Based on the aforementioned, the purpose of this thesis is to investigate, analyze, and summarize the security measures for banking transactions performed under EU PSD2 in order to provide better guidance and understanding to traditional banks and stakeholders during implementation, as well as their impact in terms of protecting transactions, data, and payment services. The study is accomplished, in particular, by examining the Guidelines (GLs) and RTS that emerge and are introduced through the EBA, as well as the applicability of the relevant legislative articles and provisions defined on the basis of Directive (EU) 2015/2366 of the European Parliament and of the Council, including the new European personal data protection framework “General Personal Data Regulation” (EU) 679/2016 (GDPR) regarding the protection of the privacy of users' personal data, as defined in the PSD2. Also, the thesis emphasizes the importance of investigating the degree of knowledge by interested parties for their correct implementation, and, by extension, the degree of their effect in assuring the security of bank transactions. In addition, it indirectly tries to highlight potential approaches to dealing with and resolving the issue of lack of harmonization and clarity of security standards and measures, in order to ensure that stakeholders make better use of the Directive compliance duties. It is expected that upon its completion, this work will contribute to the further enrichment of the subject under consideration by providing a descriptive mapping and comparison of the technical security measures, requirements, and controls provided by PSD2 to the Payment Card Industry Data Security Standard (PCI DSS) and the ISO/IEC 27001:2022 Standard, so that stakeholders will have access to a useful resource for understanding how to align security efforts to accomplish PSD2 objectives through the application of these two Standards.

Literature Review

This thesis will be focused mostly on the doctrinal research approach; it will deal with legal doctrines and conceptions while taking into account laws, regulations, cases, and other legal sources (“typical legal research”). This thesis will be based on EU-level legal sources such as legislation, directives, standards, case law, guidelines, particularly PSD2, PCI DSS, ISO/IEC 27000 series, GDPR, EBA, EDPB Guidelines, and secondary sources (e.g., books, articles) using this strategy. In this thesis, numerous academics' and institutions' references and opinions will be elaborated and examined, and the examination of the PSD2 security needs and measures will be offered while also taking into account the EBA GLs, RTS, and other official EU papers. Moreover, given the technological difficulties of contemporary online payment systems, this thesis will include some multidisciplinary insights and technical issues. Overall, the representative electronic bibliography retrieved and used includes scientific articles and published research retrieved from scientific online databases (e.g., Google Scholar), but also well-known websites that contain a wealth of information and relevant examples.

Structure

This thesis will compose of four main chapters and a conclusion. Following the introduction chapter, the first chapter will explain the PSD2's subject matter and objective, as well as the scope of its implementation, such as by providing information about relevant parties, such as TPPs and banks, to understand their interaction in the online payment sector.

The second chapter will provide an outline of the rights and obligations that banks and stakeholders must follow under PSD2. The analysis of these rights and obligations is based on the relevant legal framework for payment services in the internal market provided by the European Parliament and the Council of the Directive, as well as the EBA's RTS and GLs developed after being mandated by the respective legislative Articles.

The third and primary part of this thesis will go into detail about the applicable PSD2 security standards and measures for payment transactions, taking into account the EBA's interpretation in the relevant GLs. After analyzing the Directive's security measures, the section will explain the similarities and differences between the required security measures and controls under PCI DSS, ISO/IEC 27001:2022, and PSD2, as well as provide a mapping table illustrating the security control areas covered by each standard and the Directive.

The thesis is supposed to be completed with the discussion and conclusions as they emerge based on all the study and investigation that has occurred during the thesis.

Section 1 - PSD2: A General Overview

Objective

Introduction

Directive (EU) 2015/2366 (Payment Service Directive 2 — PSD2) provides the legal foundation for further development and improvement of multiple fields of the electronic payments within the EU [1][2]. PSD2 first aims to the modernization of the Europe's payment market through the development of innovative online and mobile payment services [4] as well as the competition within the European payments industry through a regulatory framework which encourages the emergence of new players or FinTechs in a rapidly changing market environment [12][6]. This means that the directive focuses on

contributing to a more integrated and efficient European payments market [12], which benefits both consumers and businesses since Digital Single Market and Efficient Payments Market is promoted and also more and better choices are given to customers when it comes to retail payments [4]. Therefore, the improvement of the level-playing field for PSPs is anticipated to benefit the e-commerce market because, on the one hand, it gives customers more and flexible banking and payment options to find the financial product or service which best suits their needs and, on the other hand, offers to merchants' opportunities to utilize a PSP in order to accomplish a specific purpose based on their needs a specific purpose [8][12].

For the facilitation of the new providers in the payment industry, banks will have to provide their Application Programming Interfaces (APIs) to those that request it, where consumers are expected to be able to consolidate their account information and payment options on a single device having, subsequently, better control and convenience. This is a fairly radical change, known as "Open Banking", that reinforces the EU's desire to promote increased competition and Fintech innovation [8]. Open Banking EU is concerned with banks opening their payment services to other companies, known as PSPs and TPPs, in order to build a PSD2 Directory solution to assist those providers in meeting the directive's Access to Account (XS2A) requirements and facilitating the wider aims of Open Banking. The Open Banking EU Directory Service, which was launched in January 2019, in particular, provides banks with a single, standardized reference point for accurately identifying which TPPs are authorized to access their interfaces and which roles and services they are authorized to perform on behalf of their customers. In addition, a Transparency Directory has been created to assist TPPs in understanding developer portals and ASPSPs in understanding TPP brands. Open Banking EU continues to collaborate with stakeholders on a variety of initiatives to improve understanding and collaboration among interested parties [19].

Another significant key objective of the revised Payment Services Directive is the ensuring of the customer protection through increasing the level of security of electronic payments. The PSPs must comply with specific security requirements related to Strong Customer Authentication (SCA or strong authentication hereafter) when they process payments or providing payment-related services on behalf of consumers [6].

Taking into consideration all the aforementioned, the directive establishes comprehensive and harmonized rules for payment services in the EU, intending to meet its goals and seeking to improve the existing EU rules for electronic payments [1]. The directive takes into account the emerging and innovative payment services, such as online and mobile payments and so updates the rules with the aim of ensuring high level of consumer protection, innovation and competition of the EU payments market and making international payments (withing the EU) as efficient as payments within a single country [2].

Furthermore, it is worth noting that, PSD2 brings several major benefits for customers since their rights are further protected under the revised directive. In the early 2018, the European Commission (EC) produced a "user-friendly" electronic leaflet listing consumers' rights under the directive and related EU law [1] [2]. More specifically, the Payment Service Directive aims to:

- Reduce and manage industry fraud rates without negatively impacting customer experience while increasing consumer trust.

- Develop of two-factor authentication to improve the process. PSD2 requires SCA for all European e-commerce transactions beginning on December 31, 2020 [8].
- Provide more online banking and payment options for e-commerce customers as EU payment markets open to new entrants [1][8].
- The emergence of TPPs, which will drive payments innovation and competition [8].
- Demand greater clarity and transparency in the fine print of ecommerce application licensing agreements [5].
- Reduce consumers' liability for unauthorized payments and institute an 8-week unconditional (“no questions asked”) refund right for direct debits in euros [4].
- Ensure that when a transaction is completed, card issuers make all banking funds available [5].
- Prohibit surcharging, which is the practice of charging additional fees for payments made with consumer credit or debit cards in stores or online.
- Improve the complaints procedure because it requires organizations to accept and resolve complaints in a timely manner using predefined methods [4].

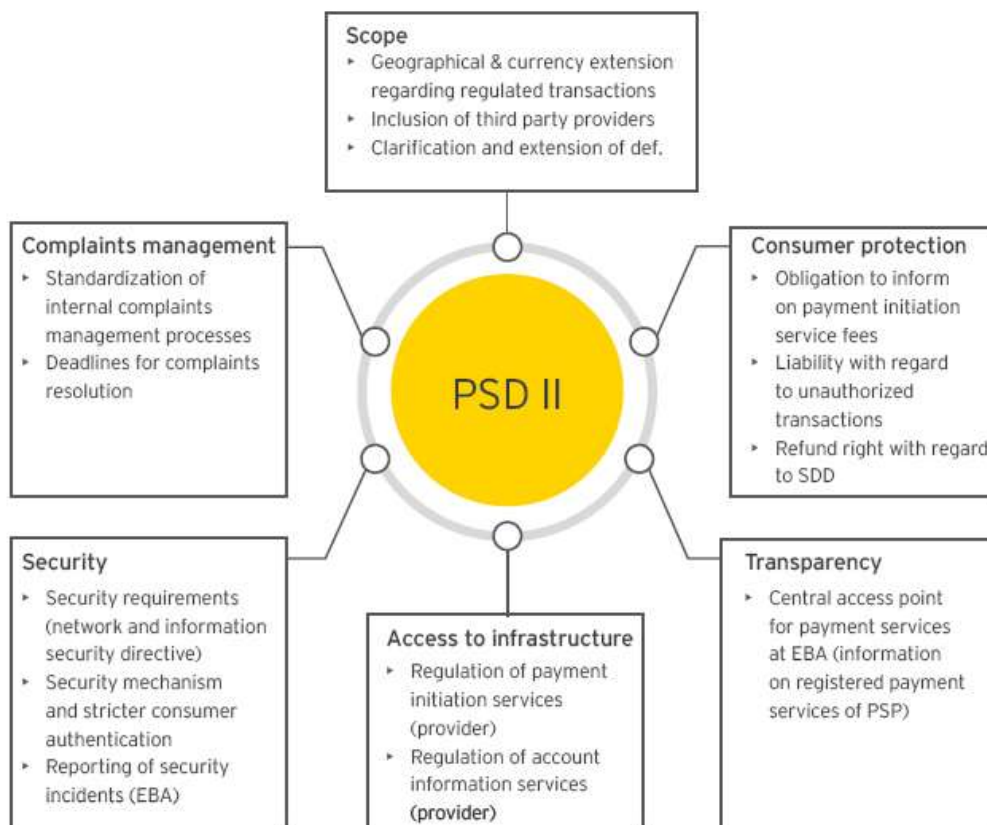


Figure 1. Objective areas of PSD2 [14]

Consumers rights

To ensure that customers' privacy is respected by all market participants and to address fraud in online payments, PSD2 introduces strict security measures for electronic payments as well as for the protection of consumers' financial data. As of September 2019, these regulations should increase consumer confidence when making purchases online [4]. The revised Directive builds on already-existing consumer protection laws to protect consumers from fraud through tightened security standards, such as the use of SCA for electronic payments [12].

PSD2 aims to encourage new entrants into EU payment markets, resulting in increased competition, greater choice, and lower prices for consumers [1][2]. Since the implementation of PSD1 in 2007, new services in the field of internet payments have emerged, in which innovative players known as FinTechs or “Third Party Providers” (TTPs or third-parties hereafter) provide specific payment solutions or services to customers. Prior to the adoption of PSD2, these FinTech companies had difficulty entering new markets because they were operating outside of the financial services’ legal framework [4]. Entering the payments market, in particular, was difficult for TPPs because many barriers prevented them from offering their solutions on a large scale and in different MSs. With these barriers removed, new players entered new markets, offering cheaper payment solutions to an increasing number of consumers across EU [11]. PSD2 now requires FinTechs to follow the same rules as traditional PSPs, including registration, licensing, and oversight by National Competent Authorities (NCAs), ensuring that they can offer their services across the EU. Due to the constant evolution of online financial services, the new rules will apply equally to traditional banks, innovative payment services, and new providers such as FinTechs. These players will now be subject to EU regulations [4], as PSD2 empowered the Commission to adopt RTS based on the EBA. They will be able to provide numerous consumer benefits. The RTS, in particular, includes two new types of payment service (PISs and AISs) [6] addressing any issues that may arise regarding the confidentiality, liability, or security of such transactions [11]. This means that providers can initiate payments on behalf of customers, provide assurance to retailers that funds are on their way, or provide an overview of available accounts and balances to their customers as of September 2019 [4]. As the world shifts away from brick-and-mortar commerce and toward a digital economy, such further integration is becoming increasingly important [11].

Moreover, PSD2 strengthens consumer rights by lowering consumers' liability for unauthorized payments and introducing an unconditional refund right for euro direct debits [4]. With improved security measures in place, consumers are better protected against fraud and other abuses and payment incidents, as previously stated. In terms of potential consumer losses, the new rules streamline and further harmonize the liability rules in the event of unauthorized transactions, ensuring enhanced protection of payment users' legitimate interests.

In addition, PSD2 reduces consumer charges and prohibits “surcharging” for card payments in the vast majority of cases (including all popular consumer debit and credit cards), both online and in stores. Surcharging is a common practice in some MSs, particularly for online payments and specific industries such as travel and hospitality. In all cases where card charges imposed on merchants are capped, merchants will no longer be allowed to surcharge consumers for using their payment card, in accordance with the complementary regulation on interchange fees for card-based payment transactions (the Interchange Fee Regulation).

Furthermore, the new Directive strengthens consumer rights when sending funds outside the EU or paying in non-EU currencies. PSD1 only addressed intra-EU transfers and was limited to the currencies of the MSs. PSD2 expanded the application of PSD1 transparency rules to “one-leg transactions”, thus covering payment transactions to persons outside the EU as far as the “EU part” of the transaction is concerned. This contributes to better information for money remitters and lowers the cost of money remittances as a result of increased market transparency [11].

Finally, the new Directive requires MSs to appoint NCAs to handle complaints from Payment Service Users (PSUs) and other interested parties, such as consumer associations, who believe their rights under the PSD2 have not been respected due to an alleged violation of the Directive. PSPs covered by the PSD2 should put in place a complaints procedure for consumers to use before seeking out-of-court redress or initiating court proceedings. The new rules require PSPs to respond to any complaint in writing within 15 business days [4].

Payment Security

The new rules outlined in the Commission Delegated Regulation (EU) 2018/389, ensure a high level of payment security. This is a critical issue for many payment users, particularly consumers who pay via the internet. PSD2 specifically requires MFA via specific identification requirements. This is primarily accomplished through APIs with identity authentication via PSD2 compliance certificates. For trusted commerce transactions on websites, these SSL/TLS certificates encrypt sensitive data and authenticate banking entities and TPPs [11]. This method of improving transaction security on both corporate and host-to-host communication systems is based on a process known as SCA [4], a new requirement that introduces specific technical standards such as PSD2-compliant certificates. The applicable requirement standards also specify when PSPs are exempt from such authentication [6]. Additionally, all PSPs, including banks, PIs, and TPPs, must demonstrate that they have in place certain security measures to ensure safe and secure payments. On a yearly basis, the PSP must assess the operational and security risks at stake, as well as the measures implemented [5].

Third-Party Access

PSD2 also introduced in a significant change in the accessibility of consumer bank account data, aggregate data, and payment data as prompted by the consumer to authorized TPPs when the customer has provided explicit consent for the granting [5][12]. In general, the Directive does not significantly alter the conditions for granting authorization to PIs in comparison to PSD1 [1]. PIs that provide payment initiation or AISs, on the other hand, will be required to have professional indemnity insurance or a comparable guarantee as a condition of authorization or registration [2]. When a payment is made, this allows larger organizations and merchants to retrieve banking industry data directly from the source, eliminating the intermediate. Many online retailers, such as Amazon, benefit from this process because it allows them to obtain additional verification of their customers' financial identities as well as instant debit resolution [5]. Consumers can manage their personal finances more efficiently by using applications that, for example, aggregate information from multiple bank accounts. Banks must establish secure communication channels to transmit data and initiate payments in order for this to be possible [4]. As a result, from the most sophisticated corporations to those who are financially excluded, new services enable customers to take greater control of their finances [12].

Implementation Scope

Payment Services

As previously stated, one of the primary goals of PSD2 is to allow consumers to benefit from more secure and innovative electronic payments. This means that the PSD2 applies to electronic payment services provided by specific entities across the EU. It is primarily concerned with electronic payments, which are less expensive than cash and also stimulate consumption and economic growth [11].

While the Commission proposed reviewing PSD1 to modernize it by taking into account new types of payment services, such as PISs, PSD2 has developed the RTS around nine different types of payment services that require a license [11] - known as a PSD2 license or PI license, as defined in Annex 1 of Directive (EU) 2015/2366 of the European Parliament and of the Council [33]. These payment services can be offered as a standalone or in any combination. The various payment services are briefly described below [11]. However, before proceeding with the description, it is important to define what is meant by payment services in PSD2. Payment services include the ability to deposit or withdraw cash from a payment account, as well as all of the operations required for the account activation. Transfers of funds, direct debits, credit transfers, and card payments are all examples of this. The Directive excludes paper transactions from its scope. Therefore, the first and most fundamental service category that RTS concentrates on is services that allow cash to be deposited into a payment account or cash withdrawals from a payment account as well as all activities necessary to operate the account [8].

PSD2 has regulated and harmonized two types of services in the context of banks opening their payment services to other companies (Open Banking), the so-called TPPs, providing consumer or business-oriented payment solutions based on access to customers' payment account through APIs. These services are PIS and AIS, also known as "new access to account (XS2A) payment services" [15]. The XS2A refers to the provision of secure access to bank accounts through APIs, allowing TPPs to provide the new services (including Card Based Payment Instruments Issuing (CBPII)) to customers [19]. Both services were already in place when the first PSD was implemented in 2007, but as a result of these changes, they have grown in popularity in recent years [15].

On the one hand, PISs initiate payment orders from a payment account held by a different provider on behalf of the user (with his prior consent). This is possible because of the open banking framework [1], which allows a payment to be initiated from the consumer's account to the merchant's account by creating an interface to bridge both accounts, filling in the information required for the bank transfer (amount of the transaction, account number, message), and notifying the store of the transaction [15]. In other words, PIS enable consumers to use online banking to make online credit transfers and immediately notify the merchant of the payment initiation. As a result, TPPs can provide immediate dispatch or real-time access to online-purchased services [8]. Credit card payments can also be made online. This payment method provides a convenient payment service. The clients must only have an online payment account, and they can use any of their accounts to make payments to a third-party from a bank's app (whether or not they belong to this entity) [11][15].

On the other hand, AIS, provide a PSU with a global overview of their financial situation at any time, allowing them to better manage their personal finances due to the easy collection and analysis of their expenses and financial needs [1] [15]. This type of information is aimed at customers and other businesses, allowing them to consolidate different payment accounts – accounts held by the user with a different provider (e.g., with one or more banks – in a single location. It also categorizes and assists clients in identifying their spending patterns based on various typologies (food, energy, rent, leisure, etc.) As a result, it aids in budgeting and financial planning [8].

One more payment service covered by PSD1 and PSD2 is the issuance of a payment instrument. Payment instruments may be issued by any authorized PSP, such as a bank or

a PI [11]. Payment instruments, in general, provide payment cards, such as debit and credit cards, as well as a variety of other personalized devices and a set of rules. The issuer and user usually agree on how to initiate payments. The agreement of the rules sets issuing between these two entities is used for payment initiation can also be characterized as another one type of payment service. PSD2 allows PSPs who do not manage the PSU's account to issue card-based payment instruments to the same account and execute card-based payments from the account managed by the PSU. Such TPPs, which act as a bank without servicing the payer's account, will be able to receive confirmation (yes/no answer after user consent) from the financial institution where the account is held, for example, whether there are sufficient funds on the account to carry out payments.

Payment transactions performed within the same provider or to an external provider are also part of the PSD2 payment services. Payment transaction executions fall into two categories. Transfers of funds on a payment account with the user's PSP or another PSP, as well as transfers of funds covered by a credit line for a PSU [8]. Execution is associated with direct debits, including one-time direct debits, payment transactions via a payment card or a similar device, and credit transfers, including standing orders, in both cases [24]. This payment permission, as well as the cash and cash withdrawals needed for a payment account operation, are related to the process of issuing a payment account to customers. PSPs can offer payment accounts to customers who have a PI license under the conditions outlined above. Customers can use TPPs payment account to perform a variety of payment activities, including depositing cash into the account, withdrawing cash, using the payment account to make purchases from retail merchants and online stores, and setting up direct debits and standing orders.

Besides, money remittance, is referred to the transfer of funds but without the creation or use of payment accounts. Money remittance, in particular, refers to a payment service in which funds are received from a payer without any payment accounts being established in the name of the payer or the payee, with the sole purpose of transferring a corresponding amount to the payee or another PSP acting on the payee's behalf [8].

Accepting and processing of payment transactions is the last example of payment service. The exchange of money over the internet as payment for goods or services ordered over the internet is referred to as online payment processing. In other words, payment processing is an electronic transaction that occurs between a company that sells a product or service online and a buyer who desires that offering. This procedure entails exchanging personal and financial information from the buyer in order to authenticate the shopper and authorize the transaction. To accept payments online, a merchant must collaborate with one or more middle partners, who handle the transaction's technology and connect to the shopper's financial institution to clear the payment. Typically, this is handled by the merchant's payment processor [3].

Stakeholders

All parties involved in the legislation are those who provide payment services in the EEA, such as all financial service providers, banks, and TPPs. In the PSD2 context, these entities are called PSPs. More specifically, A PSP is an organization that allows merchants to accept online payments such as credit card, debit card, or bank transfer (direct debit or SEPA) with or without a merchant account. PSPs are payment gateways and payment processors combined. They collaborate with banks to make it possible for merchants to accept payments [7].

According to Article 1 of PSD2, there are six categories of PSPs that are authorized to provide payment services [19]. The new Directive and its accompanying rules specify which entities are affected and which MSs must distinguish between the various types of PSPs. These are listed below:

- Credit institutions (CIs): Credit institution is defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (1), including branches within the meaning of point (17) of Article 4(1) of that Regulation where such branches are located in the Union, regardless of whether the head offices of those branches are located within the Union or, in accordance with Article 47 of PSD2 and with national law, outside the Union. A credit institution is an enterprise that receives deposits or other repayable funds from the public and grants credits for its own account, or an electronic money institution, as defined by Directive 2000/46/EC (13).
- Electronic money institutions (EMIs): Electronic money institutions are defined in point (1) of Article 2 of Directive 2009/110/EC (the Electronic Money Directive), including, in accordance with Article 8 of that Directive and national law, branches of such institutions, where such branches are located within the Union and their head offices are located outside the Union, insofar as the payment services provided by those branches are related to the issuance of electronic money [20]. According to the definition, an electronic money institution is a legal entity that is authorized to issue electronic money and manage e-money on behalf of its users. An electronic money institution can also be a PI. Each of these types of providers requires a separate authorization license [7]. All institutions in the EU that grant electronic money institution licenses adhere to Directive 2009/110/EC. This Directive serves as the legal foundation for the creation of electronic money. A company that holds an electronic money license may, in general, engage in the following activities:
 - The issuance, distribution, or refund of electronic money;
 - Payment services for e-money transactions, such as, but not limited to:
 - Cash withdrawals from payment accounts
 - Fund transfers to third parties
 - Money remittance;
 - Payment cards, which include customers withdrawing cash from a card and depositing cash to the payment card;
 - Providing account information [18].
- Post office giro institutions (in some countries): They are authorized by national law to provide payment services [20].
- Payment Institutions (PIs): A PI is any institution that provides payment services (as defined above) after being authorized to do so. A PI, in particular, is a legal person who has been granted authorization under Article 11 to provide and execute Payment Services throughout the Union. PSD2 defines two additional PI variants that can provide payment services. These are the variations:
 - Branches established by a PI in a host country that can provide payment services using the primary payment services authorizations held by their PI.
 - Agents, which are legally distinct from PIs but are contracted to perform payment services on their behalf. Agents may use the payment services authorizations of the PIs they represent or the authorizations of their registered entity. A PI may also delegate to the Agent fewer services than they hold in full as part of their payment services authorization [19].

- Central banks: The European Central Bank (ECB) and national central banks when they are not acting as monetary authorities or other public authorities.
- Government Ministries (in some countries): MSs or their regional or local authorities when not acting as public authorities [20].

Due to the new innovative payment services set out outlined in PSD2 as well as the scope expansion of existing services (payment instruments issued by PSPs that do not manage the PSU's account), new PSP definitions, known as TTPs, have emerged [11]. These new PSP players are not new categories or types; rather, they are a way of identifying entities that provide one of the new services [19]. TTPs can be app developers, financial technology (FinTech) companies and programmers, retail merchants, or even other banks [5], to whom consumers and businesses can grant access to their payment accounts and data [6]. The majority of FinTechs or TTPs are classified as PIs or electronic money institutions [7].

According to the Bank of Italy [70], FinTech refers to Financial Technology, which is defined as the provision of financing, payment, investment, and consultancy services with a high technological intensity, involving strong innovative impulses in the financial services market. FinTech evolved quickly and was divided into two categories:

- Banking services: these are businesses that compete directly with banks by offering customers alternatives to the traditional services provided by financial institutions.
- Companies that can be integrated into banking information systems to digitize processes: companies that offer “RegTech” solutions, i.e., companies that try to offer, simplify, and automate regulatory compliance processes, are an example of this category.

Below are the new regulated PSPs:

- Payment Initiation Services Providers (PISPs): This allows third-party companies to initiate payments on a consumer's behalf without requiring the consumer to visit their online bank's portal. PISPs give consumers payment flexibility while also assuring retailers that the money is on its way [8]. A practical use case would be the automatic transfer of funds to a customer's savings account [13].

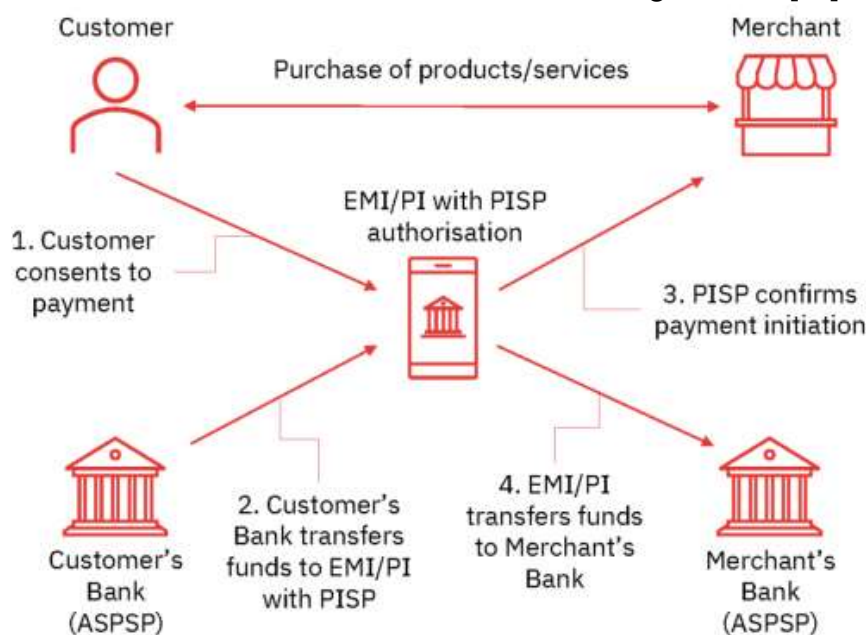


Figure 2. Illustrative role of Payment Initiation Service Provider (PISP) [121]

- **Aggregators and Account Information Service Providers (AISPs):** These are third-party companies that have access to a consumer's bank and can display account information [8]. They can request permission to connect to the bank account via an API and then provide their service using the bank account information. Having such access to such data, however, implies that you can “read-only”, i.e., these providers cannot move funds from the account [13]. An AISP, for example, allows a consumer to aggregate information from multiple accounts in a single application, providing them with a snapshot of available accounts, balances, and financial situation [8].

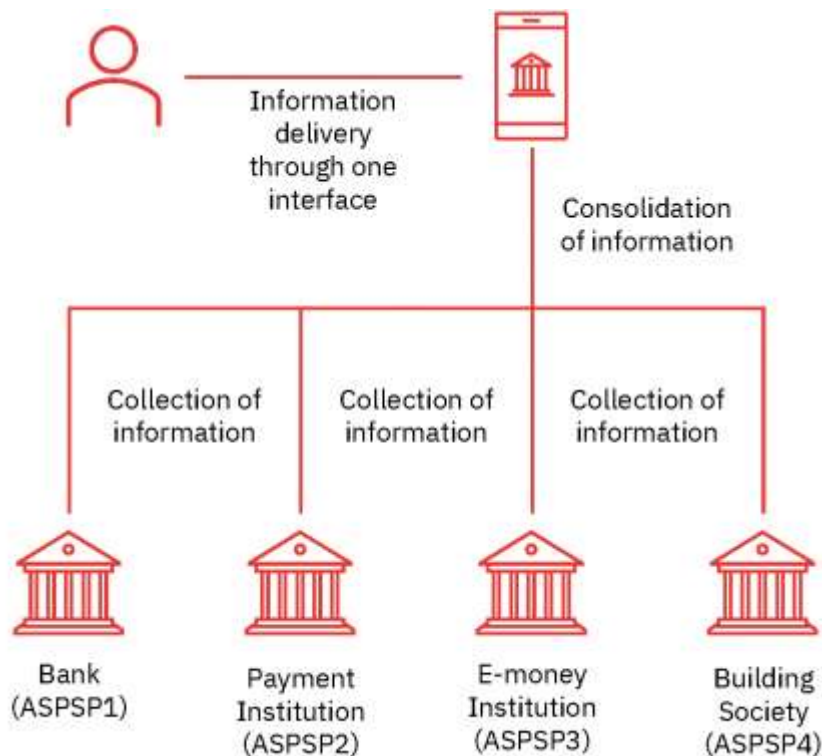


Figure 3. Illustrative role of Account Information Service Provider (AISP) [121]

It should be noted at this point that PISPs and AISPs that are already established in the market can continue to operate as PSD2 provisions allow. PSD2 specifically states that MSs must allow existing PIS or AIS providers in their territories to continue operating under the current regulatory framework [11].

- **Card Based Payment Instruments Issuing Providers (CBPIPs/CISPs/PIISPs):** Any provider who performs payment instrument issuing and/or payment transaction acquisition - CBPII services. According to Recital 67: “The issuing of a card-based payment instrument by a PSP whether a credit institution or a PI, other than the servicing the account of the customer, would provide increased competition in the market and thus more choice and a better offer for consumers”.
- **Account Servicing PSPs (ASPSPs):** To provide the new services, the aforementioned TPPs will need to rely on other PSPs to gain access to customer accounts or data. ASPSPs, which provide and operate payment accounts for PSUs, will be the primary PSPs responsible for enabling this access [19]. ASPSPs are

typically banks and other similar financial institutions, such as building societies and payment companies, that offer and maintain financial accounts with online access for their customers [16]. ASPSPs are critical components of open banking. They usually publish APIs so that customers can share their account data with TPPs so that they can initiate payments on their behalf.

- Payment Service Users (PSUs): Customers who use any of the services mentioned above [13].

According to Article 34 of the EBA’s “Regulatory Technical Standards for Strong Customer Authentication & Common Secure Communications Under PSD2” ([EBA/RTS/2017/02](#)), the new types of XS2A payment services are associated with

PSP Category (PSD2, Article 1)	→	Payment Service (PSD2, Annex 1)	→	Role (EBA RTS for SCA/CSC, Article 34)
Entity applies to be (or already is) one of the following categories...	→	PSP applies to provide one or more of the following services...	→	Once authorised, the PSP plays the following role...
• Credit Institution • E-Money Institution • Payment Institution • Central Banks • Post Office Giro Institutions (in some countries) • Government Ministries (in some countries)	→	Payment Initiation Services (PIS)	→	Payment Initiation Authorised to provide services to initiate credit transfers for customers online.
		Account Information Services (AIS)	→	Account Information Authorised to provide consolidated customer account information services online.
		Card Based Payment Instruments Issuing (CBPII)	→	Card Based Payment Instruments Authorised to provide services to issue payment instruments and/or acquire payment transactions online.
		PSPs that operate payment accounts and allow online access	→	Account Servicing Authorised to provide services to operate customer accounts, with a line of credit and payment facilities online.

Figure 4. Payment Categories, Services & Roles under PSD2 [19]

payment service roles that can only be held by the aforementioned PSP categories, depending on the XS2A services that PSPs are authorized to provide. Entities that want to provide a new XS2A service must first apply to a NCA to be categorized as a PSP and to be authorized to provide the desired payment service. If the application is approved, the PSP will be able to provide PSD2 payment services by taking on a specific role. Exempted PSPs cannot be granted authorization for PIS or AIS roles unless they first apply to become one of the permitted PSP categories [19].

Geographical scope

The PSD2 applies to “payment services provided within the Union”. PSD2 currently covers the 28 EU MSs as well as three EEA MSs (EEA, i.e., Norway, Iceland and Liechtenstein). Please keep in mind that the EU MSs’ overseas territories are not depicted on the map below. At the time of writing, the UK is still a member of the EU and must be treated as such. Should the United Kingdom leave the EU and enter the transitional period (as determined by the Withdrawal Agreement³), EU law will continue to apply, implying that the United Kingdom should be treated as an EEA state under PSD2 until the end of such a transitional period. However, it is worth noting that the future relationship between the UK and the EU is still being negotiated [22].

Country overview: in which countries will PSD2 be implemented?

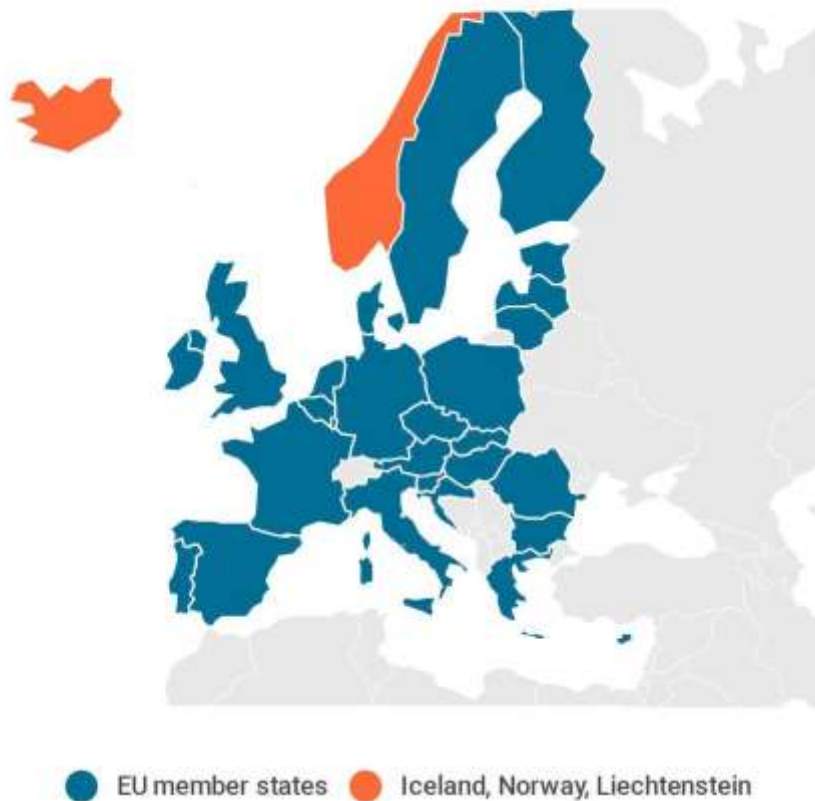


Figure 5. Geographical scope of PSD2 [22]

The legislation's requirements only apply where both the card issuer and the bank are specifically located within the EEA. However, many European financial institutions may follow the rules regardless of the merchant or customer's location. The SCA mandate essentially applies to all merchants doing business in the EEA [5].

In terms of payment transactions scope, PSD2 provisions for transparency and information, as in PSD, apply to payment transactions in a MS's currency where the PSP at both ends of the transaction is located within the EU. PSD2 expands the scope of the transparency and information requirements beyond the former Directive to transactions in any currency where only one of the PSPs is located within the EU ("one leg-out transactions"). These rules apply to the parts of the payment chain that take place within the EU [23].

Extension of the scope of PSD2

Article 2: Scope

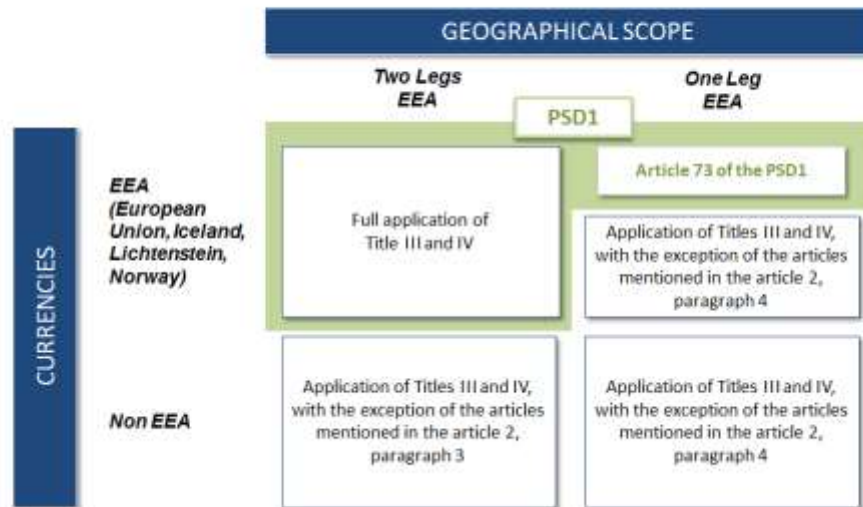


Figure 6. Expansion of payments transactions scope of PSD2 [22]

Finally, while the primary focus is on EU banks and payment processors, companies with headquarters outside the EU may be affected if they have customers or users in the EU. For example, US firms must still ensure that their EU business units are PSD2 compliant. So, if your company is thinking about expanding into the EU market, you'll need to become PSD2 compliant at some point [21].

Section 2 – Rights and Obligations

Introduction

As far as safety, convenience and security of the financial institutions' consumers are concerned, market players need specific requirements to comply with the new obligations in PSD2. To that end, the EBA has developed a set of RTS and implementing technical standards in close collaboration with the ECB (ITS). Since the implementation of PSD2 on January 13, 2016, the EBA has published a Consultation Paper (CP) with a first draft of the RTS and ITS, a set of minimum requirements which all firms, including banks acting as ASPSPs, building societies, PIs, e-money institutions, and their customers, must comply with [46] [47]. PSD2 empowered the EC to adopt the RTS draft submitted by the EBA after one year (13th January 2017), and the EC made some limited substantive amendments to this. This was done to better reflect PSD2's mandate and to provide additional clarity and certainty to all parties involved. As a result, the forced entry of the various technical requirements areas was conditional on the adoption of the RTS developed by the EBA and approved by the Commission. However, several delays in adoption and development have occurred due to delays in the transposition of the Directive into Spanish regulation and the EBA postponing the creation of technical standards to regulate third-party access and strong authentication [6]. Having said that, and in light of the potential negative impact that PSD2 implementation could have on ecommerce, PSD2 requirements began gradually entering into force on January 2018 by not all having to be implemented at the same time [8].

EBA mandates in PSD2 and their timelines

The mandates conferred on the EBA in the PSD2 will comprise six technical standards, five sets of Guidelines, and a register.

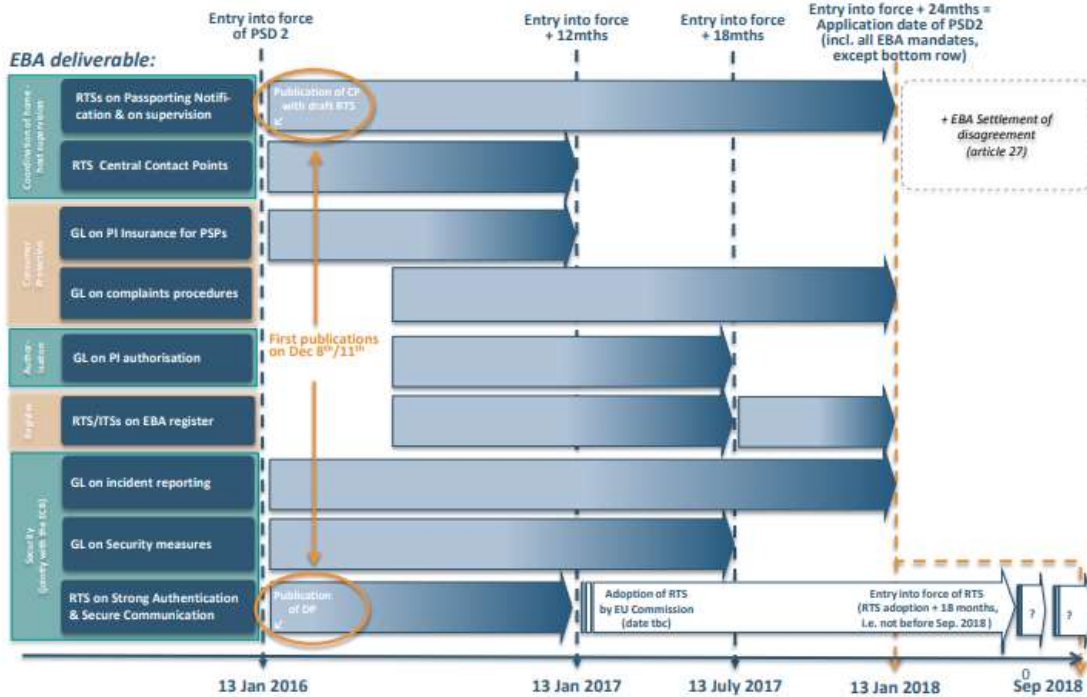


Figure 7. Technical Standards and Guidelines scope and timelines [48]

The purpose of the EBA's work is to ensure that payments across the EU are secure, simple, and efficient. As stated above, the regulatory output consists of six technical standards, five sets of GLs, and a register under the PSD2 [48].

Authorization and Registration of PIs

Application

In contrast to the PSD1, which required a license for the new entity of PI to carry out payment services, the PSD2 established information requirements for applying for a PI license as well as registering as an AISP and a PISP [13]. The PSD2 license, also known as the PI license, allows companies to PSPs in accordance with PSD2 while also allowing NCAs to better monitor and supervise the activities of these new players [11].

On November 3, 2016, the EBA issued a CP outlining its proposals for carrying out this mandate. The relevant GLs specify the type of information that applicants must submit to meet the requirements of the Directive, including:

- those in respect of the applicant's programme of operations;
- its business plan;
- the measures taken for safeguarding PSUs' funds;
- its internal control mechanisms for anti-money laundering (AML) compliance;
- the applicant's structural organization;
- the identity of statutory auditors;
- the identity of individuals with qualifying holdings; and
- the identity of the directors and persons in charge of the PI's management, as well as, where applicable, persons in charge of the PI's payment service activities.

The EBA also defined the scope of the GLs in the CP, as required by PSD2, stating that the GLs should apply to:

- applicants seeking authorization as a PI under PSD2, including applicants seeking only PISs. However, because these PIs do not acquire funds, some specific provisions of the GLs do not apply to them.
- applicants who intend to only provide AIS;
- those PSPs covered by Article 32 of PSD2 or Article 9 of Directive 2009/110/EC (EMD) who have not been exempted from all of the information requirements covered by Article 5 of PSD2, but only for those specific, non-exempted requirements;
- electronic money institutions (EMIs), as defined in Article 3(1) of Directive (EU) 2009/110, the E-Money Directive (EMD), which states that Article 5 of PSD2 applies to electronic money institutions *mutatis mutandis*.

The GLs have been divided into four different sets, the first three of which are referred to the scope of applicants as mentioned above, and the fourth one provides clarity to applicants in terms of the application's completeness. The EBA received 23 responses to its consultation, which it evaluated in order to determine which changes, if any, should be made before finalizing the GLs. The rationale section of the [EBA/GL/2017/09](#) assesses four concerns raised most frequently by respondents and also provides an exhaustive and comprehensive assessment of all comments received by the EBA from the Financial Conduct Authority (FCA). The FCA relatively published its CP on the draft authorization and reporting forms ([CP17/22](#)) in July 2017. The EBA reviewed and scored the responses, identifying a number of issues and requests for clarification from respondents. It agreed with some of their suggestions and made several changes to the draft GLs as a result. The final report of EBA GLs became effective on January 13, 2018, and was addressed to NCAs, as defined in point I of Article 4(2) of Regulation (EU) No 1093/2010, as well as the following financial institutions:

- PIs, as defined in Article 4(4) of PSD2;
- Electronic money institutions, as defined in Article 2 point (1) of Directive 2009/110/EC;
- AISPs, as defined in Article 4(19) of PSD2.

To be noted that the terms used and defined in PSD2 and Directive 2009/110/EC in the GLs have the same meaning [27] [29].

Authorization as PI & E-Money Institution

According to the EBA GLs and Article 5 of the Directive, applicants for authorization as PIs under PSD2 must meet a number of requirements in order to obtain authorization to provide e-money services and, if applicable, any payment service(s) as described above and referred to in points 1-7 of Annex I to PSD2 or service 8 in combination with other payment services. These requirements are largely consistent with PSD1. The main changes are related to PSD2's increased levels of payment security. Entities seeking authorization as a PI must submit a security policy document with their application, as well as a description of security incident management procedures, contingency procedures, and so on.

PIs that provide initiation or e-money services must be authorized, and those that provide AISs must be registered with the NCA in their “home Member State” (home MS), outlining the business plan and operating model, demonstrating appropriate levels of initial and

working capital, outlining risk management, financial controls, fraud and security monitoring, and business continuity arrangements. To cover their liabilities in this regard, PISPs and AISPs must have professional indemnity insurance or a comparable guarantee. The EBA has issued GLs on how to specify the minimum amount of professional indemnity insurance or other comparable guarantee ([EBA-GL-2017-08](#)) [22]. The relevant reference can also be found in Article 5(4) of PSD2.

The aforementioned sectors to be provided by the applicants should contain some specific information as analyzed in the section 4.1 of [EBA/GL/2017/09](#) [27]. These are mainly referred to:

- what payment or e-money services will be provided, as outlined in a business plan;
- who will be in charge of providing the services (for example, if a manager or an agent is acting on behalf of the firm);
- information on any person or firm owning 10% or more of the firm's capital or voting rights [30].

This information should be true, complete, accurate, and up to date. All applicants must follow all of the provisions in the set of GLs that apply to them. The level of detail should be proportionate to the applicant's size and internal organization, as well as the nature, scope, complexity, and riskiness of the specific service(s) that the applicant intends to provide. In any case, in accordance with the Directive, the directors and persons responsible for the management of the PI are of good repute and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organization, and the nature, scope, and complexity of its activities, as well as the duties and responsibilities of the specific position. As a result, when submitting the application form and supporting documents, the applicant should avoid making references to specific sections of internal procedures/documents. Instead, the applicant should extract the pertinent sections and submit them to the appropriate authority (CA). The application can be submitted online, on-site, or by mail, depending on the requirements of each regulator for how to submit papers. Following the submission of the documents, the regulator should review them and provide feedback, such as comments on the application [13]. If the NCAs require additional documents or clarification on the information submitted, the applicant must provide such clarification as soon as possible. All data requested under these GLs for authorizations as PIs are required for the application's assessment and will be treated by the NCA in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements and procedures on exercising the right to access, rectify, cancel, or oppose [27].

There have obviously been cases where PIs have been authorized to provide services since PSD1's inception. These PIs are permitted to continue providing payment services for 30 months (authorized institutions) or 36 months (small institutions that benefited from the PSD2 waiver under Article 26). To continue providing payment services after the transitional period, existing PIs would need to submit all relevant PSD2 information to the NCAs that have granted them their existing licenses, as well as fully comply with the relevant PSD2 requirements. Furthermore, MSs may provide for existing PIs to be granted PSD2 authorization automatically if the NCA already has evidence that the PI complies with PSD2 requirements. Before authorization is granted, NCAs must conduct a case-by-case assessment and notify the PI concerned.

According to PISPs and AISPs, because these are providers recognized as new in PSD2, existing and new providers of such services would need to apply for authorization under the PSD2 regime from the date of application of the new Directive. However, because PSD2's new security measures regarding SCA and Common Secure Communications (CSC) became applicable later than other provisions, PIS and AIS providers seeking PSD2 authorization are not required to submit proof of compliance with these security requirements until that later date. Because the provision of both types of services is dependent on the authentication procedures provided by banks, upgrades to the security requirements and procedures used by banks must be fully implemented before the PIS and AIS can be used. If banks fail to meet the security requirements and standards for secure communication on time, they cannot use this failure to impede or obstruct the use of PIS and AIS. The delayed implementation of the security requirements should not impede the provision of existing payment-related services by market players operating in MSs prior to January 13, 2016. PSD2 Article 115(5) ensures the continuity of these services. These PSPs should still apply to their national authority for the necessary PSD2 authorization as soon as possible [11].

It should be noted that, as stated in paragraph 23(d) of the EBA Opinion on the Use of eIDAS certificates, a CBPII would need to be authorized for the payment services listed in Annex I to PSD2 (*“the issuing of payment instruments and/or the acquisition of payment transactions”*), but depending on the activities it performs, its license does not necessarily need to cover the payment services listed in Annex I to PSD2 [22].

Registered Account Information Service Provider

PIs that want to provide AISs can also obtain a license as a PI that only provides AISs. Businesses that want to provide AISs in the UK can apply to become registered AISPs (RAISP). AISP providers must meet fewer conditions and have no initial capital requirements for their activities than authorized or licensed firms [13]. According to section 4.2 of the EBA GLs ([EBA/GL/2017/09](#)), these providers are applicants who intend to provide only the payment service mentioned in point 8 of Annex I to PSD2 without providing e-money services [27]. In addition, Article 33(1) of PSD2 explicitly states that:

“1. Natural or legal persons providing only the payment service as referred to in point (8) of Annex I shall be exempt from the application of the procedure and conditions set out in Sections 1 and 2, with the exception of points (a), (b), (e) to (h), (j), (l), (n), (p) and (q) of Article 5(1), Article 5(3) and Articles 14 and 15. Section 3 shall apply, with the exception of Article 23(3).” [24].

That is, AISPs are not required to be authorized by the NCA, but they must apply to be registered [22]. If the applicant intends to provide services in addition to those provided by AIS, they must apply for authorization and follow the GLs outlined in section 4.1 for PIs [27]. They are subject to prudential supervision by the NCA after registration, and they can exercise the right of establishment or the freedom to provide service in a MS other than their home MS (passporting right) if they comply with the passporting notification procedure [22]. Recital 48 explains why:

“In view of the specific nature of the activity performed and the risks connected to the provision of account information services, it is appropriate to provide for a specific prudential regime for AISPs. AISPs should be allowed to provide services on a cross-border basis, benefiting from the “passporting” rules.” [32]

As a result, information provided by applicants for registration to provide only AISs must be true, complete, accurate, and up to date. All applicants must follow all of the provisions of the set of GLs that apply to them. The level of detail required to be compliant should be proportionate to the applicant's size and internal organization, as well as the nature, scope, complexity, and riskiness of the specific service(s) to be provided. In any case, according to PSD2, the directors and persons responsible for the management of the PI are of good repute and have the necessary knowledge and experience to perform payment services, regardless of the institution's size, internal organization, and the nature, scope, and complexity of its activities, as well as the duties and responsibilities of the specific position. Furthermore, when submitting the required information, the applicant should avoid making specific references to specific sections of internal procedures/documents. Instead, the applicant should extract and provide the relevant sections to the CA. Should the NCAs require clarification on the information submitted, the applicant must provide such clarification as soon as possible. Finally, all data requested under these GLs for AISP registration are required for application assessment and will be treated by the NCA in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements and procedures on the exercise of the right to access, rectify, cancel, or oppose [27].

Assessment of application completeness

In accordance with the applications PIs should submit to be authorized or registered, the EBA issued GLs for assessing their completeness. More specifically, in section 4.4, EBA stated that an application should be deemed complete for the purposes of Article 12 of PSD2 if it contains all of the information required by the NCAs to assess the application in accordance with these GLs and Article 5 of the Directive. Article 12 expressly states:

“Within 3 months of receipt of an application or, if the application is incomplete, of all of the information required for the decision, the competent authorities shall inform the applicant whether the authorisation is granted or refused. The competent authority shall give reasons where it refuses an authorisation.” [24].

If the information provided in the application is determined to be incomplete, the NCA should send a request to the applicant, either in paper form or electronically, indicating what information is missing and giving the applicant the opportunity to submit the missing information. When the application is determined to be complete, the NCA should notify the applicant, along with the date of receipt of the complete application or, as the case may be, the date of receipt of the information that completed the application. In any case, the NCA may require the applicant to provide clarification on the information in order to evaluate the application [27]. According to Article 16 of PSD2, if any change affects the accuracy or completeness of information and evidence provided in accordance with Article 5, the PI must notify the NCAs of its home MS without undue delay [24]. This update should identify the information in question, its location within the original application, the reason the information is no longer true, accurate, or complete, the updated information, and confirmation that the rest of the information in the application is still true, accurate, and complete [27].

NCA Public Register

Another important requirement imposed by PSD2 on PIs is registration in their home MS. According to Article 14 of PSD2, each National NCA (NCA) must manage and maintain a national register that is publicly accessible (accessible online), known as “NCA Public

Register”. Every PSP in the MS country of EU and the EEA, including any agents and branches, will have their registration, payment services authorizations, passporting, and other status details recorded in each NCA Public Register. The following information should be recorded:

- authorized PIs and their representatives;
- natural and legal persons entitled to an exemption under Article 32 or 33, as well as their agents; and
- the institutions referred to in Article 2(5) that are authorized to provide payment services under national law.

It should be noted that branches of PIs must be registered in their home MS if they provide services in a MS other than their home MS.

This public register shall identify the payment services authorized by the PI or registered by the natural or legal person. Authorized PIs must be listed in the register separately from natural and legal persons who are exempt under Article 32 or 33. Furthermore, the register must be open to the public, accessible online, and updated on a regular basis. Any withdrawal of authorization and any withdrawal of an exemption pursuant to Article 32 or 33 must be recorded in the public register, and the NCAs must notify the EBA of the reasons for the withdrawal of any authorization and any exemption pursuant to Article 32 or 33 [24].

The stages of the home MS registration process applied to PIs and EMIs is depicted in the below graphical representation. It also may apply to Credit Institutions, but it may differ depending on the country.

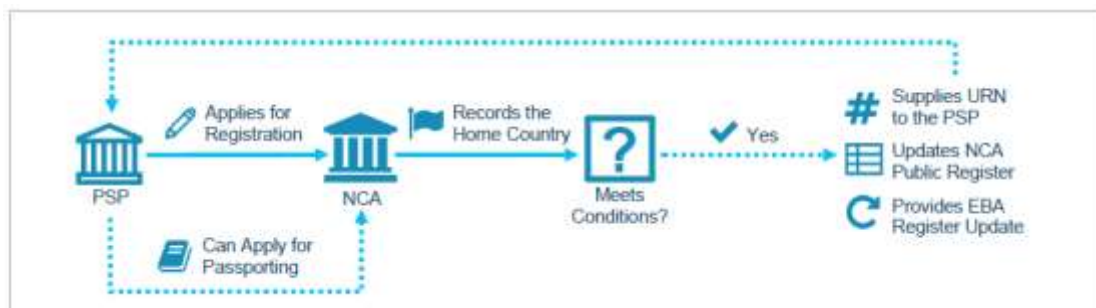


Figure 8. Registration in the home Member State (NCA Public Register) [19]

1. Application: To become a PSP, an organization must first apply to a NCA in a MS country of the EU or the EEA.
2. Home Country: The PSP's “Home Country”, as well as their principal headquarters in that MS, will be recorded by the NCA.
3. Unique Registration Number (URN): Once the PSP has met all of the conditions and requirements for their requested payment services authorizations, the NCA will issue them a Registration Number (or Authorization Number) that is specific to that NCA. The PSP's ID will be the URN, which will also record their Registration/Authorization Status, Payment Service Roles Authorized (the payment services that they are authorized to provide), and Country Permissions for Each Role Authorized (their passporting rights).
4. Passporting: If a PSP wishes to provide payment services in a country other than their home country, they must apply to the host NCA through their home NCA.

5. Registers: Pursuant to Article 14, point 3, the home NCA will update their Public Register and provide an update to the EBA Register.
6. Change Management: The home NCA will manage any changes to the PSP's Registration/Authorization Status, Payment Service Roles, or Country Permissions for Each Role Authorized, record those changes in their NCA Public Register, and provide an update to the EBA Register.

Home and Host Member State Cooperation

PIs are primarily supervised by the MS in which they are authorized to provide the defined payment services. When a PI intends to provide payment services in another MS, these activities are generally supervised by the home MS. However, if the PI provides these services through established agents or branches in the other MS (the host MS), that MS has the authority to act in the event of an infringement or suspicion of infringement of EU rules under the Directive [36].

Passporting

Some PSPs will need to register with, and apply to, their home NCA for the appropriate payment service registration or authorization in order to provide Opening Banking payment services, including any XS2A services they want to offer in the EU and EEA. Once a PSP has obtained the necessary authorizations and payment service roles, they must apply for passporting rights in order to provide the services for which they are authorized across the EU [19]. Although PSD2 supervision has not changed, a more detailed passporting procedure has been introduced to strengthen the host MS's investigative and supervisory powers. This procedure promotes improved cooperation and information exchange among national NCAs [11]. Article 29(6) of PSD2 mandates the EBA to develop draft RTS ([EBA/RTS/2018/03](#)) specifying the method, means, and details of cooperation in the supervision of cross-border PIs [36].

As set out in Article 28 of PSD2, passporting is the exercise by a business of its right to carry out activities and provide services regulated by EU legislation in another EEA State based on authorization or registration in its home EEA State. The activities can be carried out through a host-state establishment (establishment passport) or on a cross-border services basis without using a host-state establishment (cross-border service passport). PIs, PISPs, and AISPs may use PSD2 passporting rights to provide payment services in another EEA country. The definition of PIS includes services to initiate a payment order at the payer's request in relation to a payment account held at another PSP in one of the EEA States. More precisely, the payer *“has the right to make use of a PISP to obtain the service referred to in point (7) of Annex I of PSD2”* if the payment service is provided within the EEA according to article 2 of PSD2 [22].



Figure 9. Passporting application process [19]

As previously stated, any PSP that has already obtained a payment services authorization from their home NCA may reapply to provide those same services in another EU/EEA country. This passport application must go through the home NCA rather than the host country's NCA [19]. Article 28(1) specifies the types of passport applications that should be made by authorized PIs to provide their payment services in another MS [37]. Also, details of any Branches or Agents specific to the PSP for the host country should be included in the passporting application.

When a PI submits the passport application, some specific information will be transmitted or communicated by the NCAs of the home MS to the NCAs of the host MS. Specifically, the home NCA will provide the details of the passporting application to the host NCA, and the host NCA will process the application and notify the applicant of the decision within three months of receipt, as stated in Article 28(2) and (3) [19]. Moreover, point (5) mandated the EBA to develop RTS ([EBA/RTS/2016/08](#)), which specify the framework for cooperation and information exchange between the NCAs in the context of PI passport notifications [37].

Moreover, upon receiving a passport application from a PI, the NCAs of the home MS must evaluate the completeness and accuracy of the information provided in accordance with Article 28(1). The time periods referred to in the first subparagraph of Article 28(2) and the first subparagraph of Article 28(3) begin on the date of receipt of a complete and accurate passport application. If the information provided in the application is determined to be incomplete or incorrect in accordance with paragraph 1, the NCA of the home MS shall notify the PI without delay, indicating which aspects of the information are deemed incomplete or incorrect. Also, where a procedure for resolving disagreements between NCAs of different MSs has been initiated in relation to a passport application from a PI pursuant to Article 28, the NCAs of the home MS must notify the PI of the deferral of a decision on the application pending resolution under Article 19 of Regulation (EU) No 1093/2010 [37].

Should the passporting application is approved by the host NCA, the home NCA will update the home NCA Public Register, provide an update to the EBA Register, and notify the PSP of the passporting authorization (related to the URN supplied to that PSP). Otherwise, should the host NCA declines the passporting application and provides reasons for the decision, the home NCA will relay this information to the PSP and either advise on resubmission or reject the passporting application outright. There will be no updates to the home NCA Public Register or the EBA Register. The PSP can begin providing payment services in the host Country once the home NCA Public Register has been updated to reflect the successful passporting authorization. Due to the possibility of a delay, the PSP must notify their NCA when they begin payment services in the host Country.

Finally, if the payment services authorization of a home NCA is revoked:

- All associated passporting authorizations will be revoked as well.
- The home NCA will notify the host NCAs of the change in status.
- Any changes in status will be recorded in the home NCA Public Register and the EBA Register will be updated.
- The PSP will be notified by the Home NCA.

On the other hand, if a host NCA's passporting authorization is revoked:

- The host NCA will notify the home NCA and explain the decision.
- The home NCA will revoke the host Country's passporting authorization in the home NCA Public Register and EBA Register.
- The PSP will be notified by the home NCA [19].

Reporting and Central Contact Points

In addition, the host MS may request that PIs with agents and branches in its territory report on their activities on a regular basis, with the frequency of reporting specified [11]. To that end, Article 29(6) of PSD2 mandates the EBA to develop draft RTS ([EBA/RTS/2018/03](#)) outlining the means and details of any reporting requested by host MSs from PIs on payment business activities conducted in their territories through agents or branches, as well as the frequency of such reporting. According to Article 29(2), such reports “*shall be required for information or statistical purposes and, as far as the agents and branches conduct the payment business under the right of establishment, to monitor compliance with the provisions of national law transposing Titles III and IV*” of PSD2. Furthermore, according to Article 3(1) of Directive 2009/110/EC, as amended by Article 111 of PSD2, the aforementioned requirements apply to EMIs *mutatis mutandis*. As a result, the EBA issued a CP on its proposals, which ran from October 27 to January 5, 2018, and received nine responses. After reviewing the comments, the EBA decided to disregard the option considered in the CP for NCAs to require reporting from a specific subset of PIs; host NCAs must require reporting from all PIs if they decide to require periodical reporting from PIs providing payment services in their territories through agents or branches, for the reasons explained in more detail in the feedback table in section 5.2 of the final report. Finally, in response to a comment made by one of the respondents, the EBA has decided to clarify how the RTS apply *mutatis mutandis* to EMIs, particularly those EMIs that only distribute e-money in the host MS through natural or legal persons acting on their behalf [36].

As previously stated, where those PIs operate under the right of establishment, that information should be able to be used to monitor compliance with Titles III and IV in the host MS of this Directive. As a result, Article 29(4) of PSD2 states that MSs require those institutions to appoint a central contact point in their territory to facilitate supervision by NCAs of home and host MSs, including by providing documents and information on request [38][24]. This requirement achieves the goal of adequate communication and information reporting, as well as cooperation among NCAs [38]. In addition, the fourth Anti-Money Laundering Directive ([Directive EU/2015/849](#)) gives MSs the option of requesting a central contact point on their territory [40]. The establishment of such a contact point, on the other hand, can only be requested to ensure compliance with money laundering and anti-terrorist financing rules. This provision should be distinguished from the MSs option under PSD2, which can only be used by the PI to ensure adequate communication and information on PSD2 compliance [11].

In support of these provisions, Article 29(5) of PSD2 directs the EBA to create a draft RTS ([EBA/RTS/2017/09](#)) outlining the criteria to be applied when determining, in accordance with the principle of proportionality, the circumstances under which the appointment of a central contact point is appropriate, as well as the functions of those contact points, in accordance with Article 29(4) of PSD2. These draft RTS, in particular, consider:

- the total volume and value of transactions conducted by the PI in host MSs; and

- the nature of the payment services offered; and
- the total number of agents registered in the host MS.

These provisions apply to EMIs that provide cross-border payment services through agents under the right of establishment, as defined in Article 3(1) of Directive 2009/110/EC, as amended by Article 111 of PSD2. Therefore, in order to carry out this mandate, the EBA contacted NCAs in the 28 EU MSs and gathered information on cross-border payment services provided by PIs and EMIs through agents under the right of establishment. The EBA developed the criteria outlined in the draft RTS based on the mapping results and issued a CP on June 29, 2017. On September 29, 2017, the three-month consultation period ended. Four positive responses to the CP were received by the EBA [41].

Finally, because emergency situations are possible in the context of this adequate communication and information process via the contact points, appropriate measures should be taken. In particular, in emergency situations where immediate action is required to address a serious threat to the collective interests of PSUs in the host MS, such as large-scale fraud, the NCAs of the host MS should be able to take precautionary measures in parallel with cross-border cooperation between NCAs of the host and the home MS and pending measures by the NCA of the host MS. These measures must be appropriate, proportionate to the goal, non-discriminatory, and temporary, as well as properly justified. The NCAs of the relevant PI's home MS, as well as other authorities concerned, such as the Commission and EBA, should be informed in advance, or, if this is not possible due to the emergency situation, without undue delay [11] [38].

EBA Register

To improve transparency in the operation of PIs authorized by or registered with NCAs in their home MS, including their agents, and to ensure a high level of consumer protection in the Union, easy public access to the list of entities providing payment services is required. In other words, NCAs must maintain a national, publicly accessible, online, and constantly updated register of PSPs authorized to provide Opening Banking payment services, including XS2A services. Hence, PSD2 requires the EBA to create a “central register”, as explained in PSD2 recital 42 [38].

The EBA has created and maintains a central electronic register in which it publishes a list of the names of PIs, electronic money institutions, exempted PIs, exempted electronic money institutions, AISPs exempted under Article 33 of PSD2, institutions authorized to provide payment services under national law, branches, agents, and service providers as defined in Article 3(k) and (l) of PSD2. Credit institutions (which can also provide payment services such as AIS and PIS) are included in a separate EBA register. MSs must ensure that the information they provide is up to date. Article 15 PSD2 specifies the requirements for the EBA's central register.

On December 13, 2017, the EBA published the final Report on the RTS and the ITS on the EBA register for adoption by the EC (“Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2)” and “Draft Implementing Technical Standards on the details and structure of the information entered by NCAs in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366”), respectively [EBA/RTS/2017/10](#) and [EBA/ITS/2017/07](#).

These final drafts define the register's three main functional features:

- the information (i.e., which are the service providers listed and which is the related information)
- the alignment of the EBA's register in the event that the CA's register changes
- how any interested party (consumers and service providers) can gain access to and copy the register's content.

All providers authorized and/or registered in the EEA are listed in the [EBA electronic central register](#) as:

- PIs, their host-country branches, and their agents in both the home and host countries;
- AISP, as well as their branches and agents in the host MS;
- electronic money institutions, their branches in the host country, and their agents in both the home and host countries;
- natural or legal person benefiting from various exemptions (Article 32 of PSD2 and their agents, Article 9 of Directive 2009/110/EC and their agents, service providers carrying out services under points (i) and (ii) of PSD2 points (k) and (l)); [22]

The EBA Register is a compilation of all NCA Public Register data from all EU and EEA member countries. Some (but not all) of the PSPs authorized to perform XS2A services are stored in these registers. For each of the aforementioned providers listed in the EBA register, NCAs communicate to the EBA a set of information to be stored, which includes the name, the type of natural or legal person, the commercial name, the full address and country, the unique reference number (URN), the payment services for which the PI has been authorized and/or registered, the country permissions for each authorized role/service, the status and dates of granting or withdrawing authorization/registration, and which payment services it is providing or intends to provide in which host MSs. The EBA register is directly updated by the NCAs [19]. NCAs can feed and change information in the EBA register using either automatic or manual methods. In both cases, NCAs are required to enter into the electronic central register by the end of the day any changes in their national registers relating to the granting or withdrawal of authorization or registration. Once the data has been technically and automatically validated by the EBA, it is immediately published and made available; a time stamp indicates when the last change/synchronization between the EBA register and the national registers occurred.

The EBA has made a public search engine available on its website based on a set of criteria. Public users can also download the electronic central register into a machine-readable standardized file at least twice a day at pre-agreed intervals to obtain a copy of the full content. The EBA must disclose the agreed-upon intervals for such updates. However, credit institutions are not included in the EBA's electronic central register. This is because the EBA's mandate, as stated in Article 15(5) of PSD2, requires the EBA to maintain a register based on a pre-defined list of institutions, which does not include credit institutions. Banks are entered into the EBA's register of credit institutions, which is also kept up to date. Therefore, ASPSP can confirm the validity of TPP authorization/registration in both registers - the EBA register maintained under PSD2 and the EBA's credit institutions register, the latter of which contains the indication of ASPSPs acting as TPPs.

Concerning some persistent market concerns about the need for credit institutions to obtain additional authorization/registration in order to provide AIS and/or PIS, the EBA

confirmed: “all authorized credit institutions are entitled to provide the whole range of payment services, including AIS and PIS, and to do so without any need for additional authorization” (para. 26 of [EBA/RTS/2017/10](#) and [EBA/ITS/2017/07](#)) [22][24][43].

Access to Payments Systems

Another significant requirement for authorized or registered PSPs is access to payment systems. Article 35(1) of PSD2, in particular, states explicitly:

“Member States shall ensure that the rules on access of authorized or registered PSPs that are legal persons to payment systems are objective, non-discriminatory and proportionate and that they do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system.”

The criteria applicable to direct or indirect access to payment systems (non-discriminatory and proportionate) enable payment system owners to make informed decisions about direct and indirect participant access, provided that the access criteria are compliant with PSD2 Article 35. Payment systems designated under the Settlement Finality Directive (Directive 98/26/EC), as stated in paragraph 2, continue to be exempt from the requirements of Article 35(1) [22]. For the purposes of this exemption, MSs shall ensure that where a participant in a designated system allows an authorized or registered PSP that is not a participant in the system to pass transfer orders through the system, that participant shall, when requested, provide the same opportunity to other authorized or registered PSPs in an objective, proportionate, and non-discriminatory manner in line with paragraph 1 [24].

One significant difference between PSD2 and PSD1 is that the exemption from access requirements for three-party card schemes (3PS) does not apply to 3PS that operate as de facto four-party card schemes (4PS). PSD1 required traditional four-party schemes (4PS) to grant licenses to PSPs to issue cards and/or acquire transactions under “objective, non-discriminatory, and proportionate” conditions based on Article 28 of Directive 1. This access requirement did not apply to 3PS, which meant that a 3PS could choose which PSPs, if any, could participate in any part of its scheme. For example, it allowed a 3PS to operate in some EU countries in a manner similar to a 4PS (e.g., by collaborating with one or more other PSPs), while remaining purely closed in others. Furthermore, under PSD2, 3PS are still free to decide whether any PSP can participate in any part of their scheme, except where they “operate as de facto four-party card schemes, for example by relying upon licensees, agents or co-brand partners” as stated in Recital 52 PSD2.

The Court of Justice of the EU clarified the preceding in Case C-643/16, concluding that:

“a three-party payment card scheme that has entered into a co-branding agreement with a co-branding partner does not lose the benefit of the exception provided for by that provision and, therefore, is not subject to the obligation laid down in Article 35(1) of that directive in a situation where that co-branding partner is not a PSP and does not provide payment services within that scheme with respect to the co-branded products. However, a three-party payment card scheme that makes use of an agent for the purposes of supplying payment services loses the benefit of that exception and, therefore, is subject to the obligation laid down in Article 35(1).”

Furthermore, the PSD2 access requirement must be read in conjunction with Article 6 of the IFR, which states:

“Any territorial restrictions within the Union or rules with an equivalent effect in licensing agreements or in payment card scheme rules for issuing payment cards or acquiring card-based payment transactions shall be prohibited”. In other words, a PSP (for example, an acquirer) authorized to acquire 3PS transactions in one EU Member State should also be authorized to acquire those transactions in other EU Member States [22].

Access to accounts maintained with a credit institution

Access to a payment account maintained by a credit institution is critical for PIs to conduct business. PSD2 specifically states that MSs must ensure that credit institutions do not block or hinder access to payment accounts and that PIs have objective, non-discriminatory, and proportionate access to credit institutions' payment accounts services. This is especially important for money transfer services, as many of them have lost access to the banking system in recent years [11].

Article 36 of PSD2 and Recital 39 provide the appropriate relevant context and clarification. It is, specifically, explained that PSPs engaging in one or more of the services covered by PSD2

Recital 39 and Article 36 of PSD2 provide the necessary context and clarification. It is specifically stated that PSPs providing one or more of the PSD2 services *“should always hold payment accounts used exclusively for payment transactions”*. Thus, MSs *“should ensure that access to such accounts be provided in a manner that is not discriminatory and that is proportionate to the legitimate aim it intends to serve. While access can be basic, it should always be sufficiently extensive for the PI to be able to provide its services in an unobstructed and efficient way”*.

PSPs must make decisions about opening payment accounts for PIs based on an objective, non-discriminatory, and proportionate assessment that takes other legal and regulatory obligations into account, as well as due diligence. In other words, a credit institution has the right to reject PI account applications based on evidence of anti-money laundering concerns, for example. Credit institutions that refuse a PI access to a payment account must explain their decision to the appropriate authorities [22] [24].

Provision and Use of Payment Services

According to the substantive law as set forth in Title IV of PSD2, the key elements of consumer payment transactions carried out in the context of the provision and use of payment services will be examined in this section. Particularly, the common provision in Article 61 allows related parties to contract out of or vary some of the rules other than in connection with a consumer PSU. As a result, parties may agree not to:

- Article 62(1)'s provisions addressing charge allocation;
- consent through an agreement for authorization (Article 64(2));
- the notification period following an improperly or erroneously completed payment transaction (Article 71(1));
- Article 72(1)'s definition of the burden of proof in relation to an alleged unauthorized payment transaction;
- distribution of losses resulting from unauthorized payments (Article 74);
- the right to a reimbursement for debit transfers (Articles 76 and 77);
- an order for payment is irrevocable (Article 80), and;
- allocation of losses resulting from incomplete or flawed execution (Article 89).

Another common provision, not specifically mentioned, is Article 93, which provides for defense to liability under Title IV's liability provisions. In particular, Article 93 states that liability in connection with the authentication or execution of payment transactions shall not arise in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a PSP is bound by other legal obligations covered by Union or national law.

Authorization of Payment Transactions

Consent

A payment transaction is only authorized under PSD2 if the PSU has given his consent for the transaction to be carried out. Articles 64 to 77 of the Directive cover authorization, electronic authorization, onus of proof, liability for losses, and reversal of authorized debit transfers.

The execution of a payment transaction requires authorization in the form of “consent”. Article 64 only considers authorization in terms of the payer's consent, which is obviously required for “debit-pull” withdrawals from the payer's account. There is no mention of the payee's authorization given to the payee's PSP to carry out a debit transfer from the payer's account. As a result, based on Article 64, authorization may be given *“prior to or, if agreed between the payer and the PSP, after the execution of the payment transaction”* and in the form and procedure agreed upon between them [62].

Consent to execute a payment transaction must be provided in the form and manner agreed upon by the parties, typically in the framework contract (for example, by providing login and password, communicating credit card details, or scanning a QR-code and a PIN) [63]. Moreover, it may be given through the payee or the PSP. A payment transaction is considered unauthorized in the absence of such consent [62].

However, when referring to “consent”, it is first necessary to distinguish the various stages of the payment service flow, and thus the specific type of consent we are discussing. It is possible to identify the following types in particular:

- Consent for service provision (to the TPP): This is the PSU's consent to the TPP for the provision of CISP, PISP, and/or AISP services. Before providing payment services and exercising the prerogatives outlined in articles 65, 66, and 67, CISPs, PISPs, and AISPs must obtain the explicit consent of the PSU. More details on this type of consent can be found in PSD2 as well as the EBA's RTS on SCA & CSC. Recital 93 of PSD2 specifically states, *“It is necessary to set up a clear legal framework which sets out the conditions under which PISPs and AISPs can provide their services with the consent of the account holder without being required by the ASPSP to use a particular business model, whether based on direct or indirect access, for the provision of those types of services”*. It should be noted that the provision of consent may differ depending on the CISP, PISP, or AISP. For example, Recital 10 of the RTS states that *“consent can be given individually for each request of information or for each payment to be initiated or, for AISPs, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user”*. This could be some agreed-upon form, even if it is not the only one. It is critical that the forms agreed upon do not require the ASPSP to conduct “additional checks of the consent given by the PSU to the TPP”, as stated in article 32(3) of the RTS [22].

Because PSD2 does not specifically require PSUs to communicate their consent/withdrawal of consent in relation to PISs also to the ASPSP (although so), there is a risk that, if a payment is initiated by a PISP, the ASPSP may be unaware that the PSU has withdrawn his or her consent to initiate a payment or a series of payment transactions [26]. It should be noted that, according to Article 32(3) of the RTS on SCA & CSC, ASPSPs should not perform any additional checks on the PSU's consent, as this may create an impediment to TPP services.

- Consent to execute a payment (whether through a TPP or not): this refers to the PSU's authorization of the payment transaction, with or without the involvement of a PISP. As provided for in Article 64(2) PSD2, consent for payment execution can be given through the PISP. Given that payment consent *“shall be given in the form agreed between the payer and the PSP”* (see art. 64(2) PSD2) and *“in accordance with Article 80”* (see art. 64(3) PSD2), an ASPSP may include a specific provision in the contract between an ASPSP and his PSU stating the possible forms to be agreed to as well as the procedure for giving consent (see art. 64(4) PSD2). ASPSPs are required (see Art. 66(4) PSD2) to provide or make available to PISPs all information on payment transaction initiation and all information accessible to the ASPSP regarding payment transaction execution.
- Consent to access, process, and retain (store) personal data: This is the permission the PSU must give the PSP to process personal data in accordance with Article 94 of the Data Protection. In light of the General Data Protection Regulation (GDPR), this user consent is especially important if the ASPSP needs to provide account-related information. More information on personal data protection can be found in the following section of “Security Measures” [22].

Confirmation on the availability of funds

According to Article 65 plus recitals 67 and 68, it is defined as the use of a card or card-based payment instrument issued by a licensed PSP (CBPII) other than the customer's ASPSP, which allows the CBPII to seek confirmation from the ASPSP at the time of the request as to whether sufficient funds are on the account in the form of a simple “yes” or “no” answer at the time of the request [22][62]. The ASPSP should immediately notify the specific PSP card issuer of the availability of funds on the payer's payment account *“for the execution of a card-based payment transaction”*, but only if the payer/PSU has given the ASPSP prior explicit consent to respond to such PSP requests [62]. If the PSU has not provided such consent to the ASPSP in accordance with Article 65(1) PSD2, the ASPSP will be unable to provide fund confirmation to that CBPII. When consent is granted, PSUs must notify their ASPSPs and, ideally, amend or withdraw it [22]. Confirmation must be laconic; the ASPSP should not reveal the account balance and is not permitted to block funds. The PSP, for its part, may not store or use the response for any purpose other than the execution of the card-based payment transaction [62].

“This Article does not apply to payment transactions initiated through card-based instruments on which electronic money as defined by Directive 2009/110/EC is stored”, states Article 65 (6). Recital 68, for example, contends that *“given the specific nature of electronic money, it should not be possible to apply that mechanism to payment transactions initiated through card-based payment instruments on which electronic money is stored”* [22].

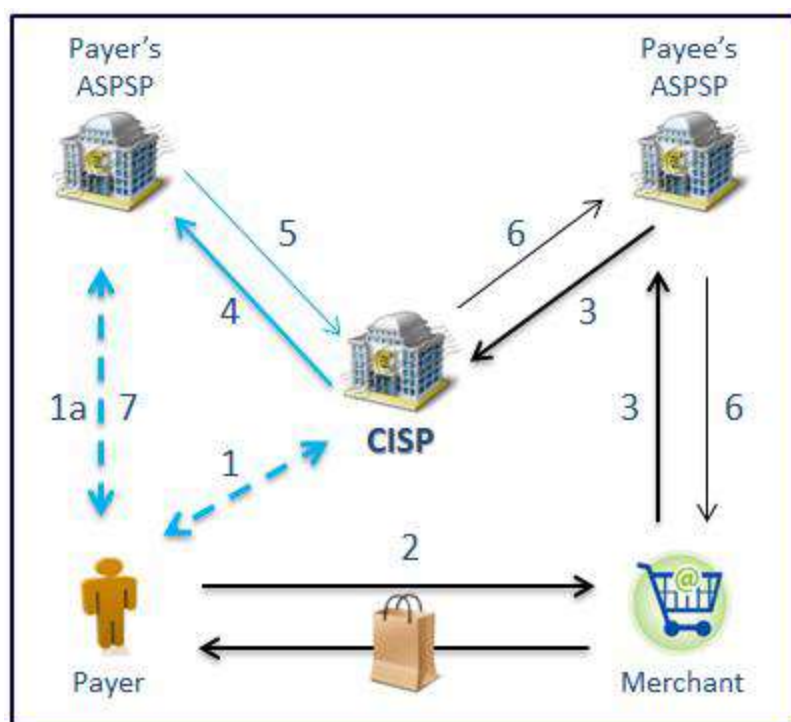


Figure 10. Payment transactions through a card-based payment instrument issuer (CBPII) [22]

Recitals 67 and 68, as well as article 65 of the PSD2, refer to the CISP operating features depicted in the figure above, which are summarized as follows:

1. The payer enters into an agreement with another PSP/CISP that provides an alternative payment card and issues the new card with specific credentials (for example, PIN code = strong authentication). (1a) The payer provides explicit consent to his ASPSP, identifying the PSP/CISP to whom the ASPSP should respond on the availability of funds if addressed.
2. The payer initiates the card payment transaction at the POS by entering his PIN code (SCA).
3. The merchant's PSP requests that the PSP/CISP who issued the payment card confirm the availability of funds.
4. The PSP/CISP requests confirmation of funds availability to the payer's ASPSP where the payer's account is located.
5. The Payer's ASPSP provides a simple Yes/No answer on fund availability. The ASPSP may not block funds on the payer's payment account based on the confirmation. The funds are settled through a direct debit transaction, for example, between the payer's ASPSP and the issuer (recital 68).
6. The PSP/CISP sends the response to the merchant via the merchant's PSP, and the card transaction at the POS can be completed or denied if sufficient funds are not available.
7. Meanwhile, if the payer requests it, his ASPSP notifies him that a request for confirmation on the availability of funds from a specific PSP/CISP has been made and the response has been provided.
8. Payment transactions initiated through card-based payment instruments that store electronic money are excluded.

Only the blue steps 1, 1a, 4, 5, and 7 in Figure 10 are required under PSD2 article 65. The article does not address the payment. Steps 2–6 are solely included to show how a third-party card-based payment instrument provider could apply the availability of funds question mentioned in Article 65. The card issuer is supposed to be issuing cards under a general purpose four party scheme in this use case example.

It should be noted that Article 65 can be used by issuers with the following business models and product setups:

- Issuers of general-purpose cards in four-party schemes.
- Card issuers in three-party schemes

Following that, the PSP pays the amount to the merchant's ASPSP upon request (payment card schemes typically debit the card issuer's account). This section is governed by the card scheme rules rather than Article 65.

In general, and as reported on recital 68 of PSD2 “the use of a card or card-based payment instrument for making a payment often triggers the generation of a message confirming availability of funds and two resulting payment transactions. The first transaction takes place between the issuer and the merchant’s ASPSP, while the second, usually a direct debit, takes place between the payer’s ASPSP and the issuer.” As a result, there must be a clear distinction between the confirmation process and the handling of any subsequent settlement transaction. Settlement, or debiting the PSU's account with its ASPSP, can take the form of a credit transfer initiated by the PSU or a direct debit (originated by the card-based payment instrument issuer). This part of the process will be governed by the standard PSD2 provisions governing payment transactions between PSPs, such as authorization, authentication, and liability. In fact, recital 68 continues stating that “Both transactions should be treated in the same way as any other equivalent transactions. PSP issuing card-based payment instruments should enjoy the same rights and should be subject to the same obligations under this Directive, regardless of whether or not they are the ASPSP of the payer, in particular in terms of responsibility (e.g., authentication) and liability vis-à-vis the different actors in the payment chain.”.

The PSD2 provisions of Articles 66(5) and 67(4), relating to PIS and AIS, explicitly state that such services shall not be “*dependent on the existence of a contractual relationship*”. Although there is no equivalent wording in Article 65, the conclusion is the same: there is no need for an agreement between the CISP and the ASPSP (although all categories of TPPs and ASPSPs are always free to negotiate agreements if they so desire) for the performance of the CISP service to the PSU [22].

Access to Payment Accounts

Articles 66 and 67 require ASPSPs to provide secure communication facilities with authorized PISPs and registered AISPs, as well as the ability to provide services to all payment accounts that are accessible online (via the internet or a mobile application downloaded onto the PSU's mobile device).

Personalized Security Credentials (PSC) should be used in conjunction with consent, security, confidentiality/data protection, bank secrecy, and fraud prevention/detection. The ASPSP is responsible for safeguarding the account information of its customers. Articles 66 (3)(b) and 67 (2)(b) must be read in conjunction with Articles 69, 70, and 97. There are currently various business models and practices in the TPP space, with some relying on the re-use of PSU's PSC and others not requiring access to these credentials and instead

operating on information flows between ASPSPs and the TPP. Article 69 (2) states, similarly to PSD1, that the PSU shall take all reasonable steps to safeguard its personal security credentials. While this provision remains in PSD2, the text does not forbid PISPs and AISPs from reusing the PSU's personalized security credentials. Recital 69 provides context: “The obligation to keep personalized credentials safe is of the utmost importance to protect the funds of the PSU and to limit the risks relating to fraud and unauthorized access to the payment account. However, terms and conditions or other obligations imposed by PSPs on the PSUs in relation to keeping PSC safe should not be drafted in a way that prevents PSUs from taking advantage of services offered by other PSPs, including PIS and AIS. Furthermore, such terms and conditions should not contain any provisions that would make it more difficult, in any way, to use the payment services of other PSPs authorized or registered pursuant to this Directive”. The possibility of using PSU's PSC is also mentioned in the RTS, subject to the security requirements outlined in Article 30.

Concerning the identification of TPPs towards ASPSPs when accessing payment accounts, Article 34 of the RTS on SCA & CSC and the EBA Opinion on the use of e-IDAS certificates under the RTS on SCA & CSC specify that for the purposes of identification, PSPs shall rely on qualified certificates for electronic seals or website authentication. All processes must be auditable and audited by independent security experts. The next section of “Security Measures” delves deeper into the various security topics surrounding the access process to payment accounts (XS2A). Furthermore, according to Article 68(5), ASPSPs may block a transaction. In addition, the ASPSP may deny an AISP or PISP access to a payment account “*for objectively justified and duly evidenced reasons*”. If the PISP cannot be identified for whatever reason, the following procedure may be used:

- If there is an issue with an electronic certificate, the PISP or AISP must contact the certificate authority to renew or obtain a valid certificate.
- If there is incorrect or incomplete information in the national register, the PISP or AISP must contact the NCA to have it corrected or updated.
- When personal security credentials (PSC) are incorrect or incomplete, the PISP or AISP must contact the PSU to complete or update the PSC.
- If access is denied due to suspected or actual PISP or AISP fraud, the ASPSP must notify the payer and the appropriate authorities.

During the “transition period”, however, the ability of an ASPSP to deny access if it cannot identify the TPP does not apply fully. According to the EBA's transition opinion from PSD1 to PSD2, “in accordance with Article 115(2), (4) and (6) PSD2 AISPs and PISPs may access customer account information without being blocked (unless there are reasonably justified and duly evidenced reasons for doing so) using existing methods, for instance ‘web scraping’ or ‘screen scraping’ (where the PSP logs in to an account as if it were the user) unless national law prevented such access before PSD2 came into force on 12 January 2016”.

In the event that the ASPSP denies a PISP or AISP access, the ASPSP is required by article 68(6) to notify the appropriate authorities [22][62].

Unauthorized payment transactions

In general, distinguishing between authorized and unauthorized payment transactions is relatively simple, at least theoretically [63]. The liability of ASPSPs has not changed as a result of PISP intermediation. However, PSD2 specifies that the PSU's “sole port of call” for rectification is the ASPSP. Thus, pursuant to Article 90 PSD2, an ASPSP shall

reimburse the PSU whenever a transaction is not executed or is executed incorrectly, even if initiated by a PISP, even if the latter is at fault. However, the PISP must then demonstrate that the transaction was authenticated, accurately recorded, and not affected by a technical breakdown within its sphere of competence. Otherwise, because the PISP initiated the payment transaction, the PISP is required to refund the ASPSP.

In the case of a PSU that denies authorizing an executed payment transaction, Article 72(2) establishes a presumption of unauthorized payment transactions because the use of a payment instrument recorded by the PSP is insufficient to prove either authorization, fraud, or the failure or gross negligence of the payment service payer. As a result, the PSP, including, where applicable, the PISP, must rebut the presumption by providing supporting evidence to prove that the transaction was authorized, correctly executed, or that there was fraud or gross negligence on the part of the PSU. The PISP will turn over this evidence to the ASPSP. The PSD2 does not specify to whom the PISP must provide this proof. We assume this is in reference to the ASPSP. However, in the absence of a contract between a PISP and an ASPSP, and given that a PSU is entitled to a refund from the ASPSP in the interest of consumer protection, it remains to be seen how the allocation of liability provisions will operate in practice. In any case, Recital 74 states that liability allocation should compel ASPSPs and PISPs to accept responsibility for their respective parts of the transaction that are under their control. ASPSPs should immediately refer the case to their supervisory authorities or courts in this case. TPPs will not be allowed to operate in the market unless they have professional indemnity insurance or a comparable guarantee, it appears. More details can be found in the EBA's "Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (PSD2)" ([EBA/GL/2017/08](#)).

The PSD2 provides no clarification on the ASPSP's recourse when the PISP denies any wrongdoing. In the absence of any authority being granted to the NCA, it is assumed that ASPSPs will be required to refer the case(s) to supervisory authorities or national courts.

Another topic addressed in the context of unauthorized payment transactions is that covered by Articles 74(1) and (2) of PSD2. Particularly, paragraph 1 states that, except in cases of fraud or gross negligence on the part of the payer, a payer may be required to pay up to EUR 50 for any unauthorized payment transactions. This maximum amount has been reduced from the previous EUR 150 PSD1 threshold. MSs may reduce this maximum amount depending on the circumstances listed in 74(1) last sentence. On the other hand, paragraph 2 states that where the payer's PSP does not require SCA and the payer has not acted fraudulently, the payer shall not bear any financial losses and introduces the liability shift principle in the context of the application of SCA. In the case of card-based payments, the financial loss is borne by the party in the payment chain that does not support SCA. In the case of card-based payments, this means that if the acquirer used one of the RTS exemptions to SCA and sent the transaction to the issuer without requesting SCA (and assuming that the issuer, who has the final say, allows that transaction to go through), the acquirer will be liable if the transaction is fraudulent. In contrast, if an acquirer supported SCA by requesting the issuer to perform the SCA, the issuer will be liable for the fraud on those transactions whether or not the issuer actually stepped up to request the cardholder to perform SCA, unless the payer acted fraudulently.

Last but not least, PSD2 has introduced a new article to address “card pre-authorizations” in response to issues identified in some MSs where card issuers can take up to several weeks to cancel pre-authorizations or release balances. This is PSD2's Article 75. When a customer makes a purchase, the card details are checked, and the purchase transaction is authorized as usual, but the transaction is set to “pre-authorized” status. Funds may be placed on hold, and the money may not be deducted from the cardholder's account at this time, but instead held until the final payment is processed. The agreement between issuers and cardholders determines whether the amount is blocked or not. According to Article 75(1), the issuer can only block an amount on the card if the cardholder has consented to the exact amount that can be blocked. Because it is the payee's responsibility to inform the payer of the amount he wishes to block on the card, the payer's ASPSP can only rely on the customer's consent to execute the transaction and thus better specify the customer's rights within the contract. The following, in particular, could be considered:

1. If the amount to be blocked is displayed on the terminal screen (this is up to the terminal provider) and the consumer enters his/her PIN to consent to the blocked amount.
2. If the merchant communicates the amount to be blocked on the card to the cardholder in the form of a POS receipt (both physical and virtual POS) and the customer signs it/enters PIN to give his/her consent to the amount to be blocked.

In most cases, the issuer will not have complete confidence that the amount was communicated to the payer by the payee (e.g., the issuer will not know for sure that the merchant operating a petrol station has placed a stick on the pump informing the cardholder of how much will be blocked on the card). The issuer must rely on merchant communication. According to Article 75(2), the card issuer must release the blocked amount without undue delay after receiving the exact amount and the payment order. As previously stated, the issuer is reliant on the merchant to provide the exact amount. Without merchant cooperation, the issuer cannot act. However, the block will not be released until the issuer receives the payment order [22][26][63].

Debit Transfers

Articles 76 and 77 add a provision dealing with a limited right for refund in connection with authorized debit transfers to the above-mentioned Article 75 analysis. Specifically, Article 76 provides for a refund to which a payer is entitled from his or her PSP for an authorized completed debit transfer, that is, a “*payment transaction which was initiated by or through the payee which has already been executed*”. Such a right is available to the payer where the authorization did not specify an exact amount for the payment transaction and its amount “exceeded the amount the payer could reasonably have expected taking into account his previous spending pattern, the conditions in his framework contract and relevant circumstances of the case.”. A framework contract governing a direct debit may waive such conditions. A framework contract, on the other hand, may state that “*the payer has no right to a refund where:*

- (a) *[he] has given his consent to execute the payment transaction directly to his [PSP]; and*
- (b) *where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least four weeks before the due date.”*

A request for a refund under Article 76 must be made within eight weeks of the debit to the payer's account, according to Article 77. Within 10 days, the payer's service provider must comply or respond [62].

Execution of Payment Transactions

This section explains the rights and obligations associated with payment transaction execution. The term “execution” isn't defined in the Directive. The term appears to denote the performance of the entire payment transaction, rather than just the carrying out of the instruction contained in the “payment order”, based on the heading of Title IV Chapter 3, which refers to the execution of the payment transaction, as well as the context elsewhere in the PSD2. The latter is the definition of “execution” in American Uniform Commercial Code (“UCC Article 4A”) [65]. At the same time, elsewhere in the Directive, reference is made to the “execution” of a “payment order”, defined in PSD2 art 4(13) to mean *“an instruction by a payer or payee to its [PSP] requesting the execution of a payment transaction”*. Hence, “execution” appears to be used inconsistently [64].

Payment Orders

Payment orders and amounts transferred are the aspects of payment transaction execution covered by PSD2 Articles 78 to 81. Articles 78 and 80 appear to treat the payer as the payment order giver. This is true for credit transfers but not for debit transfers. Indeed, Article 4(13) effectively acknowledges that the payment transaction in a debit transfer is initiated by the payee's payment order. As a result, what is communicated to the payer's PSP in a debit transfer is an instruction executing the payee's payment order issued to the payee's PSP under the payer's authority. In the context of debit transfers, “payment order” may be interpreted to refer to such communication.

Article 78(1) states that “[t]he payer’s account shall not be debited before receipt of the payment order” and defines “the time of receipt” as “when the payment order is received by the payer’s [PSP]”. The original PSD Article 64, which is the forerunner to the current PSD2 Article 78, applied to a payment order transmitted to the payer's PSP either directly by the payer (in which case it is a credit transfer) or indirectly by or through a payee. The payment transaction is a debit transfer in the latter case, where, in the usual scenario, the payee transmits the payment order to the payee's PSP for further transmission to the payer's PSP. However, the payment transaction is a credit transfer if the payee transmits the payment order directly to the payer's PSP, effectively acting as the payer's agent, rather than through the payee's PSP. Because the options were mutually exclusive, they were removed from PSD2, which in Article 78 covers all variations of payment order receipt.

Article 79 governs the refusal of payment orders. According to 79(1), a PSP who refuses to execute a payment order must notify the user of the refusal, as well as the reason for it and the procedure for correction. According to the framework contract, the user may be charged for notifying an objectively justified refusal. The PSP, for its part, does not have complete discretion over the right to refuse. According to Article 79(2), the payer's [ASPPSP] shall not refuse to execute an authorized payment order in all transfers *“[w]here all of the conditions set out in the payer’s framework contract are met, and “irrespective of whether the payment order is initiated by a payer...or through the payee,” the payer’s [ASPPSP] shall not refuse to execute an authorized payment order”*. [62].

Another point raised in the context of payment execution is the irrevocability of a payment order, which is addressed in Article 80 of PSD2. Article 61 PSD2 allows the PSP and PSU to agree that Article 80 does not apply in whole or in part. The principles governing

irrevocability have not changed in general from PSD1 to PSD2. However, the implementation of PIS has some implications in this regard. In an online/e-commerce setting, a payment order initiated by a PISP requires execution by an ASPSP. That explains why the order is not revocable under Article 80(2), except in cases covered by Article 80(5), in which the payment order may be revoked if agreed upon by the PSU and the relevant PSPs (including PISPs). Because PISPs are PSPs, article 78(2) on receipt on an agreed (future) day or the next business day, and article 80(4) on the PSU's right to revoke at the latest *“by the end of the business day preceding the agreed day”*, also apply to PISPs if they offer future transaction dates [22][26].

In addition, Article 81 addresses the amount of a payment transaction. The fundamental principle enshrined in Article 81(1) is that the full amount instructed is to be transferred, with no deductions made by the payee's service provider or any intermediary. Fees should be charged to the account and not deducted from the transferred amount. Thus, pursuant to Article 81(2), an agreed charge may be debited separately to the payee's account by his PSP rather than deducted from the amount credited. It is the service provider of the party initiating the payment transaction's responsibility, according to Article 81(3), to ensure that the payee receives the full amount of the payment transaction [62].

Execution Time and Value Date

Another issue that PSD2 is expected to address in terms of payments execution is the extent to which it regulates the time required to conduct a currency exchange at one or both ends of a payment transaction – for example, where a PSU wishes to make a payment in a currency other than the currency of the account, he/she wishes to debit, or to have a payment arriving in one currency credited to an account in another currency.

Article 82 defines the scope of application of the execution time and value dating articles (Articles 83 - 87). The types of payment transactions to which Articles 83–87 apply are mentioned throughout Article 82.

An execution time period longer than that specified in Article 83 may be agreed upon between the PSU and his/her PSP, as long as it does not exceed D+4. Non-EEA currencies are deemed to fall under the category of “other” payments, which are also subject to Article 82(2) where applicable. When funds arrive with a payee's PSP in a currency other than the payee's account currency, the payee's PSP may need to seek explicit instructions from the payee, which may take time, or may simply be unable to perform the specific currency conversion requested on the same day due to the conventions of the foreign exchange markets. Articles 82 to 87 need to be read in conjunction with Article 2. Thus, according to:

- Article 2(2) – The provisions of Articles 82 to 87 apply to intra-EEA payments made in EEA currencies.
- Article 2(3) – Articles 82 to 86 do not apply to intra-EEA payments in non-EEA currencies, but Article 87 does.
- Article 2(4) – Articles 82 to 87, with the exception of 83(1), apply to one-leg payments in any currency. However, while provisions relating to making incoming funds available and value dating apply without exception for PSPs in the EEA, Article 82(2) allows for specific agreements with PSUs beyond the scope of Article 82 (1) for the purposes of articles 84 and 85.

All payment transactions are governed by Article 87 (i.e., intra-EEA payments in both EEA and non-EEA currencies and to one-leg transactions in any currency). Articles 87(1) and (3) already applied to one leg transactions in EEA currencies for the purposes of credit and debit value dating under PSD1. The application of the debit/credit value dating rule has now been extended to non-EEA transactions, but only in the absence of currency conversion, and to intra-EEA transactions in non-EEA currencies in respect of those parts of the payments transaction that are carried out in the Union. In addition, with regard to article 87(2), the rule applies I to transactions in non-EEA currencies but only in the absence of currency conversion, (ii) to transactions in EEA currencies even if currency conversion between such currency and Euros or between two EEA currencies, and (iii) to payments performed within one PSP regardless of currency and subject to the same obligations as in point (i) and (ii).

- Credit value date: The credit value date should not be later than the business day after the amount is credited to the payee's PSP account. If the funds were credited to the payee's PSP account on a non-business day, they should be credited and made available to the payee by the next business day. Once the payee's PSP account has been credited and the PSP has received all of the detailed information required to credit the amount on the payee's account, the payee's PSP should make funds immediately available to the payee - including payments within the same PSP - where there is no currency conversion or where there is a currency conversion between the euro and a MS currency or between two MS currencies. It should be noted, however, that currency exchange transactions on the beneficiary PSP side are subject to international standards, which execute up to the D+2 horizon. Nonetheless, the PSD2 requires that any currency conversion between the euro and a MS currency or between two MS currencies applied on the beneficiary PSP's side be immediate. As a result, the beneficiary PSP must ensure that the amount of the payment transaction is immediately available to the payee. Given that this article also applies to non-EEA currency payments made between or to EEA PSPs where there is no currency conversion, it should be noted that for these types of foreign currency payments, there may be time zone restrictions, which may not allow for immediate availability of funds on the PSUs account following fund receipt by the beneficiary PSP (e.g., credit of US dollar to beneficiary PSP before PSP systems open), as it is heavily dependent on the PSP bus. The credit value date for one-leg transactions in non-EEA currencies should not be later than the business day on which the transaction's exchange value is credited to the payee's PSP account held in the Union.
- Debit value date: In all cases, the debit value date should be no earlier than when the payment transaction is debited to the payer's payment account. If a currency conversion is required on the sending side because the currency of the payment account differs from the currency of the payment transaction, the payment transaction execution process begins only after the required currency is obtained (e.g., a SEPA payment from a Danish DKK account will only be initiated once the required Euro amount is available). Therefore, the debit value date should not be earlier than the execution date (the date when the payer's account is debited) [22][26].

Non-execution and defective execution

In the case of non-execution or defective execution of a payment order initiated by or through the payee, and as stated “*without prejudice to Article 71, Article 88(2) and (3), and Article 93*”, liability is allocated as follows, based on Article 89(2):

- First and foremost, the payee's PSP “*shall be liable to the payee for correct transmission of the payment order to the [PSP] of the payer in accordance with Article 83(3),*” i.e., “*within the time limits agreed between the payee and the [PSP], enabling settlement, as far as direct debit is concerned, on the agreed due date*”.
- Second, upon becoming liable in accordance with the first step above, the payee's PSP must immediately re-transmit the payment order in question to the payer's PSP. In addition, it “*shall...be liable to the payee for handling the payment transaction in accordance with its obligations under Article 87*” and “*ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's [PSP's] account*”. As required by Article 87, the credit to the payee's PSP must be value dated “*no later than the business day on which the amount of the payment transaction is credited to the payee's [PSP]'s account*” and the payee's PSP must ensure that funds are immediately available to the payee. Furthermore, the amount at the payee's disposal must be value dated on the payee's payment account no later than the date the amount would have been value dated if the transaction had been properly executed.
- Third, if the payee's PSP is not liable as described above, the payer's PSP will become liable to the payer and refund him by posting a credit value no later than the date the amount was debited. The implicit but unstated assumption is that the failure to execute is not due to a lack of funds or any other failure on the part of the payer. Indeed, the payer's PSP is relieved of this obligation if it can demonstrate that the payee's PSP received the payment transaction amount.
- Fourth, if the payer's PSP is liable under the third step above, it shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state it would have been in had the defective payment transaction not occurred.
- Fifth, regardless of liability, the payee PSP shall, upon request, make immediate efforts to trace the payment transaction and notify the payee of the outcome. In general, Article 89(1) applies to credit transfers and Article 89(2) covers debit transfers. Nonetheless, Article 89(2) states that credit transfers initiated by the payer via the payee are covered. Indeed, depending on the architecture of a system, payment transactions initiated by the payee can be either debit or credit transfers; that is, debit transfers when routed through the payee's PSPs, and credit transfers when routed from the payee to the payer's PSP – whether directly, through a switch, or even through the payee's PSP acting merely as a communication channel. Such payment transactions initiated by the payee should be covered by Article 89(1) rather than 89(2).

Article 90 governs liability for non-execution, defective, or late execution of payment transactions initiated by the payer through the payer's PISP [62]. According to PSD2 Corrigendum Article 61, the PSP and PSU may agree that Article 90 does not apply in whole or in part. As a result, this new article is included to describe PISPs' liability in the event of payment transaction non-execution, defective, or late execution. The ASPSP must refund the amount of the unauthorized payment transaction to the payer. Unless the PISP

can demonstrate that it was not responsible for the unauthorized payment transaction, the PISP is obligated to compensate the ASPSP for the costs incurred in connection with the payer's reimbursement, as well as the amount of the unauthorized payment transaction, immediately upon the ASPSP's request. PSD2 does not define the communication and process standards for the interaction and resolution of events between ASPSPs and TPPs. The ERPB WG has proposed common business practices on standardized processes for dispute resolution between ASPSP and PISP20 [22][26].

Information and Conditions

Title III of PSD2 governs transparency of conditions and information requirements for payment services for payment transactions throughout the Union. It is intended to provide users with standardized “high level of clear information” allowing them “to make well-informed choices and be able to choose freely within the Union” while also ensuring that “[l]ow-value payment instruments should be cheap and easy-to-use alternative in the case of low-priced goods and services and should not be overburdened by excessive requirements.” [62].

In general, information requirements have not changed significantly since PSD1. However, it should be noted that the impact of concomitant EU legislation on transparency requirements (specifically, Directive 2014/92/EU of 23rd July 2014 on the comparability of fees related to payment accounts, payment account switching, and access to payment accounts with basic features, the so-called Payment Accounts Directive “PAD”), as well as the ensuing level 2 rules such as the EBA standardized Union level terms and definitions, will have to be taken into account.

Returning to PSD2, the introduction of PISPs has a number of implications in Title III. The overall goal of the information requirement, as stated in recitals 54-56, remains largely unchanged, though information must now be not only necessary and sufficient, but also understandable (recital 54), and presented in a standard format (previously referred to as “manner”, recital 56). From the standpoint of ASPSPs, the review of information requirements should aim to make the PSU aware about the distinct roles and services of the ASPSP as opposed to PISPs and AISPs.

However, recitals 63 and 64 are worth mentioning because they appear to impose new restrictions on (changes to) the framework contract's terms and conditions. Recital 63 states that MSs should be able to “*maintain or introduce restrictions or prohibitions on unilateral changes in the terms of a framework contract, for example, if there is no justified reason for such a change*” in the interest of the consumer.

Furthermore, PSD2 clarifies through Article 41 that the PSP bears the burden of proof regarding its compliance with the information requirements. While MSs could previously choose to place the burden of proof for Title III compliance on PSPs, this is now a requirement. This also applies to AISPs, according to Article 33(2), even though they are generally “treated” as PIs, as stated in the same article. Additionally, Article 42(1) specifies the payment instrument and electronic money thresholds below which information requirements are waived: only individual payment transactions that do not exceed EUR 30 or that have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time. These limits have not changed since PSD1 [22][26].

Single Payment Transactions

Because the term “single payment transaction” is undefined, it must be interpreted to mean an isolated or one-time payment transaction, or better, any payment transaction not governed by a framework contract [62].

To start with, Article 44(1) referred to “Prior general information” has been amended to highlight that the PSP only needs to provide information and conditions pertaining to its own services. As a result, aside from providing general information about the PSD2's regulation of two new types of payment services (PIS and AIS) and setting out provisions regarding confirmation of fund availability in connection with card-based payment instruments (see Article 65), ASPSPs are not required to describe the specific services that TPPs may provide. The information must now be presented in an easily accessible format.

On the other hand, Article 45 has been amended to reflect the inclusion of PISPs within the Directive's scope. Article 45(1), point a) specifies that a payment order may be initiated or executed. As a result, the requirements of Article 45(1) apply to PISPs as well. Article 44 defines information on charges and exchange rates as those imposed by the PSP on the PSU. Charges must be clearly stated in accordance with Article 45(1)(c), with a clear distinction and separation of the various amounts corresponding to each transaction or service that gives rise to the specific charges.

Article 45(2) specifies the additional information that PISPs must provide to the payer, including the name of the NCA and its contact information. Because PISPs will most likely have a framework contract with the payee but a one-time or very ad hoc relationship with the payer, this is critical information for PISPs. AISPs are also subject to this article, according to article 33(2). AISPs, on the other hand, will almost certainly enter into a framework contract with the PSU. PSD2 (Article 45 (1c)), like PSD1, does not define what is meant by all charges payable by the PSU to the PSP and, where applicable, a breakdown of those charges. The goal of this article is to provide PSUs with as much transparency as possible about the charges they will be required to pay under PAD.

Pursuant to Article 46, PISPs need to make available to the payer and, when applicable, to the payee information beyond that is specified in Article 45, which includes confirmation of the initiation, a reference and the amount of the transaction and the amount and breakdown of any charges payable to the PISP. A PISP may instruct the ASPSP to send a payment from a PSU's account on the PSU's behalf. The payment must be processed at the same level of service as if the user had initiated it directly (Article 66, (4c)). The requirement to provide the payment transaction reference must be viewed within the context of broader communication between ASPSPs and PISPs (see article 66). We assume that the transaction reference mentioned in articles 46 and 47 is the same reference. The PISP provides services to both the PSU and the ASPSP.

Additionally, based on Articles 48 and 49, the PSP should provide information for the payer immediately after receipt of the payment order as well as for the payee after execution of the payment transaction. Both articles, however, have been amended to clarify that each PSP is only required to provide information about its own services [22][26].

Framework contract

A “framework contract”, as defined in Article 4(21), is *“a payment service contract that governs the future execution of individual and successive payment transactions and may contain the obligation and conditions for opening a payment account”*. To align with the

new initiation services (via which the order could be initiated), the content of the framework contract listed in article 52 has been both modified and expanded in comparison to PSD1. Thus, the PSP will have to check the current terms and conditions of their framework contracts to ensure that the contractual content is aligned with the new provisions. According to Article 33(2), AISP's are also subject to this article. While AISP's do not initiate or execute transactions (and thus are not covered by, for example, 52(2)(d) and 52(2)(e)), they will almost certainly enter into a framework contract with the PSU and should provide the PSU with the relevant information, including name and contact details, relevant NCA, a description of the relevant service, relevant charges, conditions for changing or terminating the framework contract, security measures, and communication channels.

PSD2 introduces a number of information-sharing obligations in Article 52, which PSPs must incorporate into the framework contract:

- 52(2)(g): The PSU's right under Article 8 of the Interchange Fee Regulation in the case of co-badged card-based payment instruments.
- 52(3)(a): An additional requirement to include information on charges related to *“the manner in and frequency with which information under this Directive is provided or made available”*. It is unclear how this relates to the obligation on PSPs under article 40(2) and (3) to *“not charge the PSU for providing information”*.
- 52(5b): A requirement has been added that the framework contract include information on the secure procedure (for example, to prevent phishing/social engineering) for notifying the customer by the PSP in the event of suspected or actual fraud or security threats. As a result, all framework contracts will need to be updated by ASPSPs to include this new procedure.
- According to the EBA's GLs on Security Measures for Operational and Security Risks in Payment Services ([EBA/GL/2017/17](#)), the following is stated:
 - GL 9.2 states that *“as new threats and vulnerabilities emerge, the assistance and guidance provided to PSUs should be updated, and changes should be communicated to the PSU”*.
 - GL 9.6 state that *“PSPs should keep PSUs informed about updates in security procedures that affect PSUs in the provision of payment services”, and*
 - GL 9.7 state that *“PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. PSUs should be properly informed about how to obtain such assistance”*.

Any changes to the framework contract or the information and conditions specified in Article 52 must be proposed by the PSP in the same manner as specified in Article 51(1), no later than two months before their proposed date of application. The PSU is deemed to have accepted changes unless he notifies the PSP that he does not accept them before the date of their entry into force, provided that the changes are related to areas specified in the framework contract as per article 52(6)(a). However, the PSU now has the right to terminate the contract without penalty and with immediate effect until the date when the changes would have taken effect. Hence, the PSU is given the authority to decide when to terminate the contract (before the changes take effect). The PSP should provide information on changes in easily understandable words and in clear and comprehensible form, in the

language of the state where the services are offered or in another language agreed upon by the parties, on a durable medium.

The rules governing the termination of the framework contract remain largely unchanged. However, the period after which the framework contract can be terminated for free has been reduced from 12 to 6 months.

Finally, while the content of the information for the payer on individual payment transactions must remain unchanged, a new mandatory provision must be inserted in the framework contract, according to Article 57 of the information for the payer on individual payment transactions. This provision allows the user (when acting as the payer) to choose between a monthly report of payment transactions and information on individual transactions under article 57(1) [22][26].

Currency

The issue of currency conversion services is addressed by Article 59 PSD2. This article includes a new reference to currency conversion services available at ATMs (in addition to transactions at the point of sale). This means that the party providing the payer with a currency conversion service at an ATM must disclose all charges as well as the exchange rate to be used for converting the payment transaction. The same should be true for currency conversion at the POS. [22][26].

Charges

Another piece of legislation introduced under the PSD2 is the increased transparency of bank charges to European customers. PSD2 mandates that all payments sent and received within the EU be processed as shared payment charges [22].

Previously, when sending payments within the EEA and selecting “Payee pays all charges”, the remitting bank added an additional agents’ fee to cover any intermediary/beneficiary bank charges. This fee was deducted from Payers’ bank account. With the implementation of PSD2, when a payment is sent, the charges are automatically changed to “SHARED”, which means that separate charges are taken directly by the handling banks and no claim is made to the paying bank for the agents’ fee. As a result, whenever a payment is made to a beneficiary in the EEA, it is always released as “SHARED” charges. Any bank charges incurred by the recipient must be treated as an expense, or the recipient must contact their bank directly to negotiate a refund [66].

The PSP was required to apply the sharing of charges principle only to intra-EEA payments in EEA currencies and “*where a payment transaction does not involve any currency conversion*” under PSD1. However, the scope has been broadened under PSD2 (see Article 2(3)). Article 62(2) of Directive (EU) 2015/2366 specifically states:

“Member States shall require that for payment transactions provided within the Union, where both the payer’s and the payee’s PSPs are, or the sole PSP in the payment transaction is, located therein, the payee pays the charges levied by his PSP, and the payer pays the charges levied by his PSP.”

As a result, whether or not there is a currency conversion, the article now applies to all intra-EEA transactions in all currencies. However, according to Article 2(4), this article does not apply to one-leg transactions, regardless of currency, and thus charges in this case can be applied arbitrarily: for example, SHA, OUR, and BEN options are permitted.

Article 62(2) should be read in conjunction with the full amount principle enshrined in Article 81. More specifically:

- The principle of charge sharing applies only to two-leg transactions in all currencies.
- The full amount principle only applies to two legs-transactions in EEA currencies (subject to the exceptions stated in articles 2(3) and 2(4)).

As a result, the full amount principle of Article 81 does not apply and cannot be guaranteed for intra-EEA payment transactions in non-EEA currencies with the SHA option, because intermediary institutions (some of which must be located outside the EEA) may deduct charges from the amount transferred.

Continuing with Article 62, paragraph 3 is subject to full PSD2 scope enlargement and therefore for all transactions in all currencies, in case of surcharge, the payer can be requested to pay the charges applied by the payee (e.g., the merchant) for accepting a given payment method, provided that these charges cannot exceed the direct costs borne by the payee for the use of the specific payment instrument. Payees may therefore apply surcharges, with the exception of payment instruments capped under the Interchange Fee Regulation (as defined in Article 62(4)) in the case of two legs-transactions regardless of currency (as defined in Article 2(4)). Surcharging is also prohibited for the payee when it comes to payment services covered by the SEPA Regulation (Regulation (EU) No 260/2012), such as SEPA Direct Debit and SEPA Credit Transfers.

Payees are always free to offer discounts or otherwise steer use of a given payment instrument through means other than surcharging (see also Article 10 IFR as regards card-based payments). Furthermore, PSD2 allows MSs to impose a broader surcharging ban. The majority of MSs have chosen to use that option and outright prohibit surcharging on all transactions. However, a few MSs maintained the partial ban provided for in PSD2, which may result in different client experiences across the EEA.

In the cases of additional charges or reductions, PSD2 also defines some regulations on the information should be provided either by the payee or the PSP. In particular, under Articles 60 (1) and (2):

- *“Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction.”;*
- *“Where, for the use of a given payment instrument, the PSP or another party involved in the transaction requests a charge, it shall inform the payment service user thereof prior to the initiation of the payment transaction.”*

Therefore, in comparison to PSD1, the reference to a third-party has now been changed to *“another party involved in the payment transaction”*, to account for the possibility of a PISP being involved in the transaction.

In addition, Article 60(3) includes a new provision requiring the payer to pay only the charges imposed by the payee, a PSP, or another party involved in a transaction if their full amount was disclosed prior to the initiation of the payment transaction. Because such charges are frequently calculated as a percentage of the payment amount, this provision should be regarded as fulfilled if the prior information refers to such percentages rather than the absolute amount [22].

Dispute Resolution

Last but not least, a new article has also been added in the context of the PSD2 introduction, which deals with the resolution of PSU complaints concerning all of the aforementioned rights and obligations. Article 101 specifically states that PSPs must have complaint resolution procedures in place that apply in every MS where the PSP offers payment services, in the official language of the relevant MS (or any one official language if there are several), or in another language if agreed upon between the PSP and the PSU.

A PSP's overall deadline to resolve a complaint is 15 business days (or, up to a total of 35 business days if there is a delay for reasons beyond the control of the PSP, and the PSP indicates the reasons for delay and the date for a final reply). MSs can provide for faster resolution (MS option).

The PSP shall notify the PSU of at least one out-of-court redress entity that is competent to deal with disputes arising under Titles III and IV of PSD2. PSPs must make this information easily accessible on their websites and at their branches (if they have them), as well as in their general terms and conditions [22].

Section 3 - Security Measures

Introduction

With the implementation of the PSD2, many opportunities and advantages were introduced by stimulating innovation and promoting competition within the Payments sector, while the main changes concern the market expansion for PSPs and the application of new technology and authentication mechanisms to access payment accounts (XS2A). However, due to the fact that TPP services increasingly rely on the use of personal and financial data, and because the various parties are becoming more and more reliant on IT infrastructure, security risks are increasing. Those risks may be found in data sharing with TPPs, fraud cases involving dishonorable TPPs or hacked customers, requests made via TPPs that may be vulnerable to third-party fraud powered by malware or social engineering techniques, and fraudsters who may use TPPs as an obfuscation layer to confuse banks' fraud defenses. As a result, security risks affect all PSPs, such as banks, payment gateways, and acquirers, as well as PSUs, such as individuals, organizations, and governmental bodies.

To that end, the EBA responded on December 12, 2017, based on the mandate based in Article 95 of PSD2, by introducing a set of GLs ([EBA-GL-2017-17](#)) where PSD2 requires PSPs to establish a framework with appropriate mitigation measures and control mechanisms to manage those operational and security risks raised by the payment services they provide (hereafter “risk management framework”). These measures must be proportionate to the security risks involved. PSPs must establish and maintain effective incident management procedures, including those for detecting and classifying major operational and security incidents, as part of that risk management framework [93]. In addition, a regular reporting mechanism should be established to ensure that PSPs provide the NCAs with an up-to-date assessment of their security risks and the measures they have taken in response to those risks on a regular basis [84].

However, these GLs are aimed at PSPs and only apply to their payment services, despite the fact that they are applicable to a broader range of institutions. As a result, they have been drafted to address a broader range of financial institutions under the EBA's jurisdiction, namely credit institutions that previously fell under the scope of the GLs on security measures for their payment services but now fall under the scope of these GLs for

all activities, as well as investment firms. The “Guidelines on ICT and security risk management” ([EBA/GL/2019/04](#)) outline how financial institutions should manage the information and communication technology (ICT) and security risks to which they are exposed, as well as providing them with a better understanding of supervisory expectations for ICT and security risk management. It should be noted that the term “ICT and security risks” arose as a result of the electronic nature of payment services delivered through ICT systems [94].

These GLs are one of three security-related mandates granted to the EBA by PSD2, and they were developed in close collaboration with the ECB. Access to accounts, as well as the initiation and execution of internet payments, are subject to additional control and security measures through the use of SCA and CSC channels [93]. Certain PSD2 RTS on SCA and CSC ([EBA/RTS/2017/02](#)) were published in the Official Journal of the EU on March 13, 2018 and took effect on September 14, 2019. During the transition period, PSPs could already provide their services under PSD2, but they were not legally required to implement the necessary security measures. In addition to the RTS, the EBA issued an Opinion on June 13, 2018 to seek clarification in a number of areas related to the implementation of the RTS on SCA and CSC ([EBA-Op-2018-04](#)). The RTS, in particular, contains rules on SCA and CSC, as well as a number of exemptions/exceptions that PSPs (i.e., the payer's and payee's PSPs) may invoke in order to avoid performing SCA on a given action [22].

On the one hand, these SCA and CSC security measures include the issuance and use of SCA solutions, which enable authorization to be dynamically linked to the specific amount and payee [84]. SCA, in essence, allows payments to be made more securely by requiring higher levels of authentication when completing a transaction. PSPs must implement SCA processes for customers who access their accounts online, initiate electronic payments, or conduct transactions via remote channels. Because these activities carry a high level of risk, PSD2 requires PSPs to implement appropriate security processes to reduce the likelihood of risk. Adopting appropriate SCA processes promotes user confidentiality, ensures the integrity of PSUs' PSC, and ensures communication between participants regarding transactions taking place on any particular platform [85]. PSPs must also use adequate transaction and device monitoring mechanisms to detect potentially unusual payment patterns. On the other hand, PSD2 requires the use of open and CSC standards in the context of security measures. Specifically, a standardized and dependable access interface to payment accounts (i.e., an application programming interface, API) should be provided so that, as secure identification of TPPs is permitted, so is related communication between all parties involved [54].

Banks can reduce the risk of security attacks on payment transactions by following an API architectural approach with more layers of fraud protection and authentication because they can integrate security features like access control and threat detection directly into data-sharing offerings, allowing them to be proactive rather than reactive [85]. With market agreement on a single technical specification, all systems in EU can eventually be based on one or a few technical API standards [54].

The PSD2 security mandates conferred on the EBA are finally supplemented by the PSD2 major incident reporting GLs ([EBA-GL-2017-10](#)), which were published on July 27, 2017. To minimize impact to users, other PSPs, or payment systems, such as a significant disruption of a payment system, PSPs must be required to report major security incidents to the appropriate authorities as soon as possible. When a PSP becomes aware of a major

operational or security incident, it should first notify its supervising authority, and then notify its customers if the event affects their financial interests [84]. Further details will be provided in the relevant section.

Taking everything into account, it is concluded that the PSD2 security obligations can be divided into the three major topics mentioned above. Thus, this section will explain and provide a clear analysis of which IT security measures and controls should be in place for PSPs and users to be risk tolerant in the context of managing operational and security risks, authentication and secure communication, and incident reporting [85].

Furthermore, this section is expected to be completed with a descriptive mapping and comparison of the technical security measures, requirements, and controls provided by PSD2 to the Payment Card Industry Data Security Standard (PCI DSS) and the ISO/IEC 27001:2022 Standard. This examination will highlight the differences, pros and cons, and potential parallels and gaps between both Standards and the Directive, as well as their interoperability, degree of support for one over the other, and ability to be combined. As a result, banks and organizations will have a better understanding of the solutions available to them for information security, risk management, and data protection. Banks could also be informed about the extent of their effective PSD2 compliance by implementing the two examined Standards, allowing them to achieve efficiencies in their existing processes and controls. Finally, this investigation will produce results indicating (i) which PSD2 requirements are covered by the implementation of ISO/IEC 27001:2022 and PCI DSS, (ii) which are not covered, and/ or (iii) which could potentially need further enhancement and improvement.

Common and Secure Open Standards of Communication (CSC)

The introduction of the XS2A had significant implications for the relationship between PSPs, banks, and customers/users across EU. From 14 March 2019, ASPSPs must make available to TPPs the technical specifications of their access interfaces (whether dedicated or user-facing), as well as a testing facility to conduct trials of the software and applications TPPs will use to provide services to their users. PSD2 has specified the requirements of CSC standards to be met by all relevant PSPs in order to ensure effective and secure communication between the relevant actors in the context of AIS, PIS, and confirmation on the availability of funds provided by the XS2A interfaces.

While Directive (EU) 2015/2366's Articles 65, 66, 67, 97, and 98 detail the general requirements for third-party XS2A service provision, the EBA's RTS for SCA & CSC examines the specific implementation requirements and conditions. They specifically state that ASPSPs that provide online payment accounts to payers must have at least one interface in place that meets the following requirements:

- They must be designed, developed, and implemented in accordance with specific security standards.
- Providers must use customer authentication in the case of PIS or AIS usage.
- PIS or AIS provision requires secure communication.
- Secure identification of AISP, PISP, and PSP to the ASPSP
- Protection of sensitive payment customer data exchanged.

The following sub-sections examine all of the aforementioned security specifications, also emphasizing their implementation as required by the PSD2 articles and GLs [86].

Open Banking API Standardization

The Internet already allows ASPSPs to offer their services digitally through publicly available infrastructure and digital ports. This has become so common in recent years that practically every ASPSP in the EU now offers both Internet and mobile payment services. These services, however, were previously only available to existing customers with accounts managed by their ASPSP via their Controlled Access Points, devices, and Graphic User Interfaces (GUIs), such as websites and mobile apps. The PSD2 permits new TPPs to access account services from ASPSPs via APIs. [95].

The API option has numerous benefits. Open APIs, which enable one company's products and services to be interconnected with those of others, are an important step forward in service provision and can help generate innovative services that benefit both customers and the businesses involved. As a result, industry participants would be wise to use Open APIs as soon as possible. Investing in APIs based on common standards, in particular, has advantages over both direct access and proprietary APIs. These interfaces will be less expensive to implement for ASPSPs. Given the EU's encouragement of the development of common standards, obtaining compliance confirmation may be easier if this path is taken. Finally, this course will most likely encourage TPPs to adapt to using standardized APIs, which have a wider reach than either direct access or a proprietary interface [83].

In accordance with the aforementioned, PSD2 established a new business model known as “Open Banking”. Because a secure environment has now been introduced, the Open Banking model achieved through the use of APIs contributes to ensuring and improving security in the sharing of customers' bank information with the various TPPs. Open Banking API technology, which defines how software should communicate, is the accepted standard for securely sharing and embedding data in an online environment [87]. API is a standardized protocol that allows computer programs to communicate with one another. Prior to PSD2, PISPs and AISP could use the users' online banking channel, and they collected and used the same information available to users via a method known as “screen scraping”. This was a type of technology and the practical solution used by AISP and PISP prior to PSD2 to access the users' data, as the user, without identifying itself to the bank, to provide their online payment services, because they would not have a legal right to request access to their users' banking data from the users' banks [88].

Now, PSD2 requires all banks to allow TPPs access to account information and PISs if the user has explicitly authorized the TPP to initiate such requests and the TPP is registered with the competent financial authority of its home country [87]. This is accomplished through the use of a dedicated interface, in which ASPSPs grant TPPs access to their customers' accounts via a route designed specifically for them. In practice, big part of the industry is preparing to do so through the use of Open APIs. Alternatively, ASPSPs may provide direct access in the form of “screen scraping” by simply enhancing their webpage to show only the PSD2-compliant parts and providing TPPs access to these. TPPs must, of course, be able to identify themselves in this case, and ASPSPs must be able to ensure that only PSD2-compliant content is shared with TPPs. Making this route successful will undoubtedly necessitate significant adaptation work to any pre-existing customer-facing interface – yet it will not provide the additional benefits that APIs do [83].

Taking all above into consideration, PSD2 has introduced a number of new security and control requirements, technical specifications, testing capabilities, and clear legal and operational conditions under which it can be used.

The following are the main requirements that will be examined and analyzed in relation to the secure implementation of the open banking interfaces between ASPSP, PISP, and AISP:

- Adoption of a specific “Model Data for System Interoperability” in accordance with the ISO 20022 standard advocated by the EBA.
- Guaranteeing ASPSP's direct provision of service levels and related support to its customers.
- Availability and consistency of the information set provided to ASPSP customers by the PISP and AISP interfaces.
- Limitation on the information requests placed by the users through the AISP applications usage [89].

Communication interface

To begin with, a bank that provides its customers with online access to their payment accounts is required by the EBA's SCA & CSC RTS to have at least one interface in place that allows PSPs to access the accounts. According to article 31, the bank has the option of creating a separate “dedicated” interface for PSPs or allowing them to use the user interface. Even if the bank chooses the latter option, the user interface cannot be simply opened to PSPs [86]. Pursuant to article 30(1) of the RTS, the interface must enable secure communication with AISPs, PISPs, and PSPs that issue card-based payment instruments. The aforementioned providers should also be able to identify themselves to the ASPSP via the interface.

The dedicated interface or the adapted user interface shall allow AISPs and PISPs to rely on the authentication procedures provided by the AISP to the PSU for PSU authentication. The interface must specifically allow a PISP or an AISP to instruct the ASPSP to begin authentication. Throughout the authentication, communication sessions between the ASPSP, PISP, AISP, and PSU must be established and maintained. Furthermore, the PISP or AISP must ensure the integrity and confidentiality of PSC and authentication codes transmitted by or through them.

Banks or ASPSPs must ensure that their interface(s) adhere to communication standards issued by international or European standardization organizations. To that end, it should be ensured that the technical specification of the interface is documented and, at the very least, freely available upon request by authorized PISPs, AISPs, and PSPs issuing card-based payment instruments or having applied for the relevant authorization with their NCAs. This documentation shall specify a set of routines, protocols, and tools required by PISPs, AISPs, and PSPs issuing card-based payment instruments in order for their software and applications to interact with the ASPSPs' systems. Finally, the latter must make the documentation summary publicly available on their website. In addition, ASPSPs must ensure that, except in emergency situations, any change to the technical specification of their interface is made available in advance to authorized PISPs, AISPs, and PSPs issuing card-based payment instruments (or PSPs that have applied with their NCAs for the relevant authorization) as soon as possible and no less than three months before the change is implemented. PSPs should also document emergency situations in which changes were made and make the documentation available to NCAs upon request.

Last but not least, ASPSPs must provide a testing facility, including support, for authorized PISPs, AISP, and PSPs issuing card-based payment instruments, or PSPs that have applied for the relevant authorization, to test their software and applications used to provide a payment service to users. The testing facility shall not be used to share any sensitive information [92].

Dedicated Interface

According to article 27(2) of the EBA's SCA & CSC RTS, ASPSPs that have implemented a dedicated interface. To ensure PSUs' right to use PISPs and the respective services enabling access to account information, as referred to in Articles 66 and 67 of PSD2, it is necessary to require that the dedicated interface have the same service level as the interface available to the PSU, including the same level of contingency measures. To that end, ASPSPs must monitor the availability and performance of the dedicated interface and provide the resulting statistics to the appropriate authorities upon request. In addition, if the dedicated interface does not operate at the same level of availability and performance as the interface made available to the ASPSP's user when accessing its payment account online, the ASPSP must report it to the CAs, restore the level of service for this interface case without undue delay, and take any action necessary to prevent its recurrence. The report must include the reasons for the deficiency as well as the steps taken to restore the required level of service. Furthermore, after reporting to the ASPSP, PSPs that use the dedicated interface offered by the latter may also report to the NCAs any deficiencies in the level of availability and performance required of the interface.

Furthermore, ASPSPs should ensure that the dedicated interface for financial messaging uses ISO 20022 elements, components, or approved message definitions [92]. At this point, it seems appropriate to review the most important aspects of this standard in terms of the XS2A interface. ISO 20022 is an international standard developed by the ISO Technical Committee TC68 Financial Services that is widely used in the payments sector, both between and within MSs. It is divided into several parts and describes a common platform for the development of messages⁵ for the financial services industry. It includes a syntax-independent meta model, a corresponding UML profile, modeling GLs, requirements for the generation of XML (eXtensible Markup Language) schemata and ASN.1 (Abstract Syntax Notation One) modules, and a large catalogue of messages for various financial sector business domains, including payments.

Among the various payment-related messages, the following two appear to be particularly pertinent to PSD2:

- **CreditorPaymentActivationRequestV06** (pain.013.001.06), because it contains structures for the payer (Dbtr), the payment account (DbtrAcct), the payment receiver (Cdtr), the account of the recipient (CdtrAcct), the purpose (Purp) and the amount (Amt), as required for Article 66 PSD2, and;
- **BankToCustomerAccountReportV06** (camt.052.001.06), because it allows to address accounts (Acct), to specify time periods (FrToDt) and account report structures (Rpt) as required for Article 67 PSD2 [90].

This scenario, similar to what was achieved for SEPA systems, results in the adoption of structured data models for XS2A systems (Access To Account) in the PSD2 perimeter, which is structured in three levels:

- Process Level: A description of the operational processes and the information used to support them (facilitates the identification of the information contained in the communication between the parties).
- Logical Level: The set of expected data is defined.
- Physical Level: A physical representation of the logic level's messages, based on a specific syntax and a specific standard message [89].

Finally, ASPSPs have to include a strategy and plans for contingency measures in the design of the dedicated interface in the event of an unplanned outage of the interface and system breakdown. The strategy must include communication plans to notify PSPs who use the dedicated interface in the event of a breakdown, measures to restore the system to normal operation, and a description of alternative options PSPs can use during the unplanned downtime [92].

TTP User Management

ASPSPs must allow legitimate TPPs to access their accounts without any contracts or barriers. To protect their customer resources and infrastructure, ASPSPs must treat all unknown entities as potential malicious actors until they can verify the entity's identity and validate their regulatory access. To avoid potential threats such as Denial of Service (DoS), data loss, or privilege elevation, solutions that keep the ASPSP secure while granting XS2A API access to authorized third parties are required. Given the seriousness of these threats and their consequences for ASPSPs and customer resources, ASPSPs should be able to identify a TPP each time they attempt to connect, as well as block unknown entities, or provide access to known and trusted TPPs with valid access credentials.

Controlled Access

The ASPSPs should implement some controlled access measures in order to accomplish the aforementioned actions. To be more specific:

- An ASPSP will be able to manage TPP access to systems using a User Management System (UMS).
- Automation and self-service will handle each TPP access request efficiently and cost-effectively.
- Guides and tutorials will explain the controlled access process and provide TPPs with examples.
- Support will assist TPPs when they run into errors or other issues.

First of all, a TPP can gain access to an XS2A API via the Controlled Access Point (CAP), which is developed and provided by the ASPSP. The CAP is frequently found on the Developer Portal and should be easily accessible via the Internet, complete with instructions on how to access it. The ASPSP can provide two channels at the CAP:

- The first channel is for new TPPs who are accessing the ASPSP's systems for the first time and must identify themselves.
- The second channel is for known TPPs who have previously identified themselves and been assigned a unique access identifier that the ASPSP recognizes and can allow that TPP access to the ASPSP systems to which they are authorized.

In order for the onboarding process of new TPPs requiring access to their customer accounts to offer PSD2 services to be performed safely and securely, the ASPSPs may build a UMS comprised of the following key steps and capabilities:

1. Creation of a unique identity for specific TPPs and distribution of access credentials.
2. Assigning Access Rights to Resources/Scopes for Each TPP through the issuance of additional area-specific access credentials.
3. Keeping track of previously issued TPP access credentials.
4. When a TPP returns, compare it to the issued TPP access credentials record to enable authorized access.
5. Monitoring and logging of all TPP activity, including timestamps, areas accessed, and actions taken on the TPP's behalf.
6. Management of a TPP's access credentials and rights, including changes and removal.

In case the aforementioned UMS capabilities are implemented correctly, the ASPSP should be able to identify, track, log, and control all TPP access events to the ASPSP's systems. These system records and logs could be used for the following security practices:

- Reporting automation (internal and regulatory).
- User access management, such as the removal of redundant users or the change of credentials.
- Manual user access control, such as suspending or revoking access in the event of a security breach.
- Notifications to users via their stored TPP communication details.
- Investigation and dispute resolution, in which access records (as well as any other information) of a TPP involved must be reviewed.

Moreover, as previously noted, ASPSPs can create both automatic and self-service CAPs. The CAP and UMS can both be configured as automated PSD2 functions, removing the requirement for human operators to individually examine and manage each TPP access request. This lowers costs while increasing the ASPSP's processing capacity. On the one hand, if the UMS is automated from the ASPSP side, the TPP is in charge of the requests and information input required to gain access to the ASPSP's systems. As a result, the TPP must have self-service capabilities, including a User Interface for the TPP's human operator (an Administrator) to complete an initial setup and configure their access, as well as manage the access credentials that have been issued by the ASPSP. On the other hand, by eliminating the need for the TPP to interact with a human operator on the ASPSP side, the service can be made available outside of normal working hours.

For the end user, a self-service capability may include the following activities:

- Create a User Profile (or Account).
- Assigning the User Profile to an Administrator.
- Linking Access Rights requests to the User Profile.
- The creation and deletion of user sub-profiles.
- User Sub-Profile management, including delegation or restriction of inherited access rights from the User Profile, as well as self-service for sub-users.
- Obtaining and storing access credentials.
- Access credential management, including requests for voluntary access removal and changes.
- Profile recovery in the event that the User Profile is blocked or compromised.

Furthermore, if TPPs are to be automated and provided with self-service capabilities, tutorials are required to explain the process steps involved and to provide examples of what is required of a TPP to complete the process. These may include written text, diagrams, images, and even interactive videos. However, it is up to each ASPSP to determine the appropriate level of guidance.

In addition, while the TPP will successfully operate the majority of self-service activities, there may be times when they find it difficult to complete an activity or encounter errors that they cannot resolve on their own. In these cases, there will still be a need for human-operated support and interaction, such as a Helpdesk Support team accessible via the ASPSP's normal communication channels. The ASPSP should include clear methods and details in their CAP so that the TPP can request assistance when necessary. Human operators should be given some Administrator control over the UMS and will require procedural guides to ensure that the correct ASPSP security procedures are followed for each support request.

The Figure 11 below depicts the typical user journey for an entity signing up for an API on the Internet. It is written specifically from the perspective of the TPP. The two orange boxes represent the new steps used in a PSD2 XS2A context to meet the additional identification and regulatory permissions verification requirements, and thus incorporate the fact that these APIs are not “Open”, but are restricted to specific regulated entities.



Figure 11. Onboarding for TPPs to XS2A API access [95]

TPP Identification

The process of verifying a TPP's identity and access rights is described in some detail in the EBA's RTS for SCA & CSC under PSD2. However, it requires further development in order to be fully robust and secure during implementation, while ensuring that TPPs only need to meet the bare minimum of requirements and processes. Fundamentally, in order to grant XS2A API access, the ASPSP must verify two (2) things:

- TPP identity, which means that the entity requesting XS2A services must be who it claims to be.
- Regulatory Validation in terms of which EU countries the TPP is authorized to operate PSD2 services in, as well as which PSD2 services the TPP is authorized to operate and/or access.

The use of cryptography in modern computing allows information to be bound at the source, so that the encrypted information cannot be changed or altered. Certificates are the end result of this process. Using a PKI, the owners/holders of such certificates can also use secret information that only they should have to uniquely sign a request that proves they are the correct owner/subject of that certificate. Using this model, an ASPSP can request proof of identification from the TPP and ensure that they are who they say they are [95].

The RTS provide a clear explanation referring to the certificates' usage as well as the specific certificate types that should be used per case in Article 34. PSPs must use qualified certificates for electronic seals as defined in Article 3(30) of Regulation (EU) No 910/2014 or website authentication as defined in Article 3(39) of that Regulation [91]. “Electronic Seal” refers to an electronic signature used by a legal entity to certify electronic documents as genuine, whereas Qualified Trust Service Provider refers to the legal entity that provides secure digital services and issues qualified digital certificates recognized throughout the EU (QTSP). Because the required TPP identification could only take place with certificates for website authentication (if the ASPSP initiated the connection setup or “called back” the requesting TPP), it is clear that qualified certificates for electronic seals are required for TPP identification [90].

In particular, the use of Qualified Certificates must be standardized for PSD2 in accordance with the e-IDAS regulation. All PSPs and PSUs can be compliant and provide identification, confidentiality, authenticity/integrity, and non-repudiation by utilizing e-IDAS-conformant Trust Services and the appropriate technological protocols. For website authentication, Qualified Website Certificates (QWACs) should be used so that ASPSPs and TPPs can be certain of each other's identities. QWACs, in fact, provide a method for authenticating “Internet Entity Identity” and encrypting communications to ensure confidentiality. They are designed to be used at the Transport Layer with specific protocols for Transport Layer Security (TLS) or Mutual Authentication/Transport Layer Security (MA/TLS) and are not intended to be used at the Application Layer. The proper use of TLS or MA/TLS effectively prevents any “listeners” from seeing the messages being exchanged between the two parties and ensures the confidentiality of the communication session between the two parties, in accordance with EBA’s RTS under PSD2 requirements. The Figure 12, below, shows the use of QWAC in the PSU authentication through website.

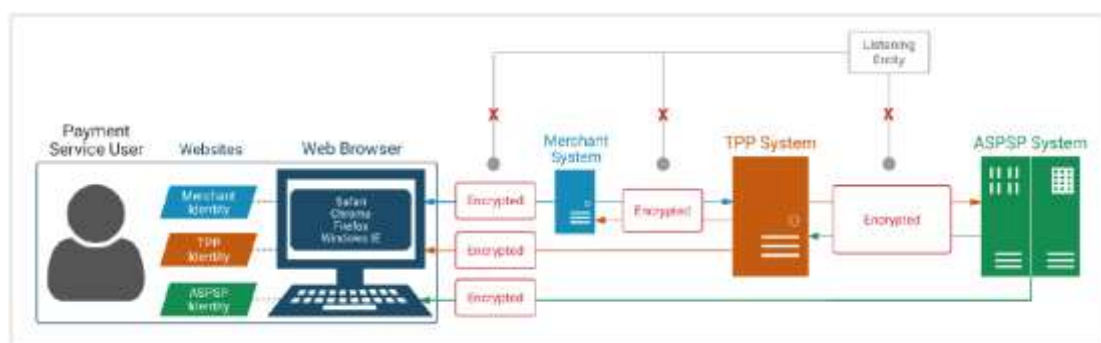


Figure 12. Qualified Website Authentication Certificates (QWACs) [95]

Instead, the Qualified Electronic Seal Certificates (QSEALCs) are not intended to be used for “Internet Entity Identity” or confidentiality at the Transport Layer for Transport Layer Security (TLS) or Mutual Authentication/Transport Layer Security (MA/TLS). A QSEALC can be used at the Application Layer, with messages passing between communicating parties to prove the origin, authenticity, and integrity that the data comes from the intended party. More specifically, once a TPP is granted API access based on their authorized payment services and passporting rights, the TPP can conduct PIS, AIS, and CBPII and must sign each API message with the Digital Signature associated with the original TPP QSEALC that was provided, as well as a timestamp for each API message as required in the RTS. This ensures that the TPP is authenticating the message it is passing to the ASPSP and can later be used as a legal proof record by the ASPSP.

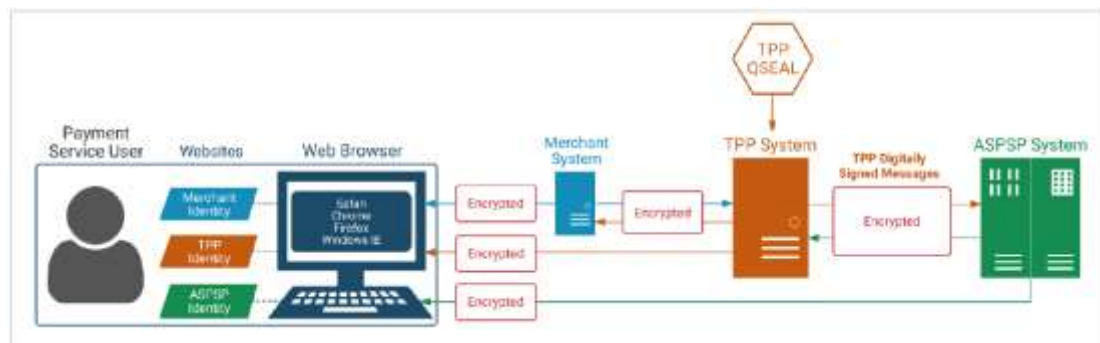


Figure 13. QSEALCs proof for Authenticity & Integrity of Transaction Messages signed by TPP [95]

The ASPSP should also use their QSEALC to sign any API messages returned to the TPP, so that the TPP is assured of the message's authenticity/integrity and can use it as a record of legal proof later [82].

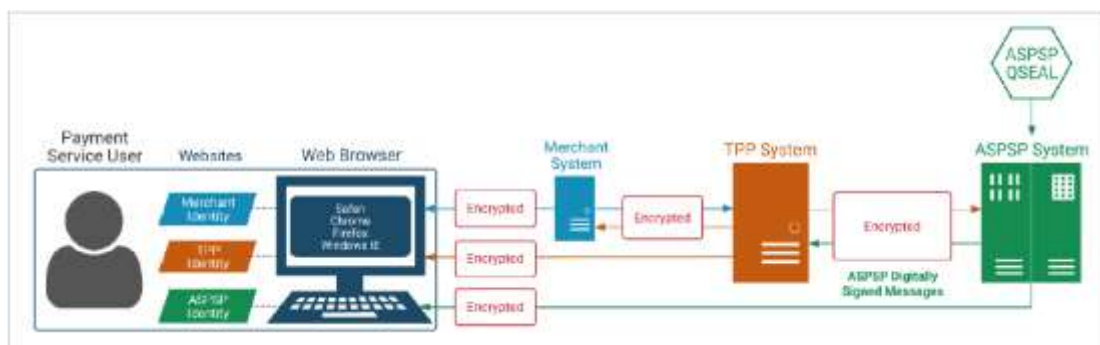


Figure 14. QSEALCs proof for Authenticity & Integrity of Transaction Messages signed by ASPSP [95]

Furthermore, because the PSD2 requirements for SCA & CSC require information about the “Legal Persons Owner” of that certificate, this certificate can be used to establish the PSD2 “Financial Entity Identity” (as opposed to the “Internet Entity Identity” in the QWAC). As stated in previous sections, the term “Financial Entity Identity” refers to the requirement of ASPSPs to be able to validate TPPs' regulatory access levels with the trusted regulatory source of NCA Public Register. To prevent malicious actors from gaining unauthorized access, such a validation service should be as standard and secure as possible. This validation can be carried out directly with the NCA or via a Trusted Service. However, not all NCA Public Registers contain the same information or are easily machine readable. This may cause problems with TPP checking by the ASPSP and may necessitate human intervention, which will significantly delay TPP access [95]. According to Article 34 of the EBA's RTS, the registration number as referred to in the official records in accordance with Annex III (C) of Regulation (EU) No 910/2014 shall be the authorization number of the PSP issuing card-based payment instruments, the AISP and PISP, including ASPSPs providing such services, available in the home MS's public register pursuant to Article 14 of PSD2 or resulting from notifications of every authorization [92]. In case, a TPP cannot prove its identity or does not have sufficient regulatory permissions, the ASPSP should deny access to it until it can be properly checked [95].

Finally, QSEALCs or QWACs must include additional specific attributes in English that do not affect certificate interoperability or recognition. These qualities are as follows:

- the PSP's role, which could be one or more of the following: ASPSP; PISP; AISP; PSP issuing card-based payment instruments.
- the name of the NCAs where the PSP is registered [91] [92].

Implementation Process Flow

Taking all of this into account, it is important to describe an overview of the process flow that should be realized once a TPP entity needs to access an XS2A API, which should be appropriately identified by the ASPSP.

To begin, once a TPP has logged into the relevant API, it can view all of the APIs and Services provided by the ASPSP under PSD2, as well as request that a new API/Service be added to its user profile. The TPP can also request that access to XS2A services be added to its profile. To that end, the TPP should normally be prompted to upload their QSEALC details, as well as sign an ASPSP generated variable, to demonstrate that the TPP is the owner (or authorized by the certificate owner) of that certificate. The UMS will then save the QSEALC details as well as the TPP's Public Key to a secure Trust Store within the ASPSP and begin the PSD2 validation process.

In the context of TPP identity verification, the ASPSP must check the following:

- Ownership: That the PKI Signature associated with the QSEALC has a matching outcome. This confirms that the TPP has access to the certificate's Private Key, proving that they are the owner. This check can be performed locally between the TPP and the ASPSP.
- Certificate Status: The Qualified Trust Service Provider (QTSP) issuing the certificate verifies that the QSEALC is valid and has not been revoked. This check can be performed by either:
 - Examining a previously downloaded local Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) List by the ASPSP, or
 - Using an OCSP Responder to contact the QTSP Issuer directly online (as specified in the QSEAL Certificate Profile information).

In either case, a Service Agreement from a QTSP Aggregator or PRETA is required.

If the identity validation fails, a log record is created and the request is rejected. The rejection should be communicated to the TPP, along with any relevant information. It is up to the ASPSP's own security policies to define any additional actions or cases that may be required, such as multiple failed attempts by a TPP using several revoked certificates in quick succession. Furthermore, if the TPP's identity is valid, a check around what that TPP is allowed to do, i.e., a PSD2 Access Check, can be performed using the following reference numbers:

- Unique Reference Number (URN): The QSEALC will include the name of the NCA as well as the URN of the TPP provided by that NCA. This URN can be extracted by the ASPSP from the QSEALC.
- Global Unique Reference Number (GURN): The ASPSP can generate a GURN that is unique across EU by using the correct combination of Country, NCA Name, and URN.

The ASPSP can use the URN or GURN to check directly with the NCA Public Register for record details under that TPP URN, or against the PRETA Open Banking EU Directory for details against that TPP URN.

Finally, if all of the aforementioned checks are successful, the TPP should be notified and shown the list of permissions available to them for the ASPSP [95].

Secure Communication Session

As previously stated in previous sections, it is critical for PISPs and AISP to use CSC standards and practices when communicating with the entity that provides the user's payment account (i.e., the bank) [7]. The establishment of secure communication among the relevant provider entities, on the other hand, allows AISP to securely request and receive information on one or more designated payment accounts and associated payment transactions, and PISP to safely initiate a payment order from the payer's payment account and receive information on the initiation and execution of payment transactions.

According to article 30 of the EBA's SCA & CSC RTS, ASPSPs, PSPs issuing card-based payment instruments, AISP, and PISP must ensure that, when exchanging data via the internet, secure encryption is used between the communicating parties throughout the respective communication session to safeguard the confidentiality and integrity of the data, using strong and widely recognized encryption techniques [91] [92]. By establishing Transmission Control Protocols (TCP) and Open Systems Interconnection (OSI) Protocols, which can be used in combination at various network layers of the XS2A Communications Infrastructure, internet communication sessions over the XS2A and Internet banking can also maximize their security and maintain their stability and interoperability [82].

In addition, PSPs issuing card-based payment instruments, AISP, and PISP must keep ASPSP access sessions as short as possible and actively terminate the session with the relevant ASPSP as soon as the requested action is completed. AISP and PISP must ensure that when maintaining parallel network sessions with the ASPSP, those sessions are securely linked to relevant sessions established with the PSU(s), to avoid the possibility of any message or information communicated between them being misrouted.

Furthermore, it is critical that the providers of AIS, PIS, and CBPII, as well as the ASPSPs, include unambiguous references to each of the following items:

- the PSU or users, as well as the corresponding communication session, to distinguish multiple requests from the same PSU or users;
- the uniquely identified payment transaction initiated for PIS;
- for confirmation of fund availability, the uniquely identified request related to the amount required for the card-based payment transaction.

Last but not least, AISP, PISP, and PSP that issue card-based payment instruments must ensure that PSC and authentication codes are not readable by any staff at any time. AISP, PISP issuing card-based payment instruments, and PISP shall promptly notify the payment services user associated with them and the issuer of the PSC if the confidentiality of PSC within their sphere of competence is breached [91] [92].

Data Exchanges

To access payment accounts and statement details, as well as other account information held by banks and ASPSPs, traditional PSPs typically need to share and exchange certain data with those TPPs under PSD2. To that end, EBA has dedicated a section of the SCA & CSC RTS to addressing the issue of data exchanges, so that ASPSPs are aware of the specific requirements with which they must comply.

To begin, they must provide AISPs with the same information from designated payment accounts and associated payment transactions that the PSU makes available when directly requesting account information, provided that this information does not include sensitive payment data. Similarly, the same information should be provided to PISPs as soon as the payment order is received. When the transaction is initiated directly by the PSU, this information refers to the initiation and execution of the payment transaction provided or made available to it. PISPs must now provide ASPSPs with the same information that the PSU requests when initiating the payment transaction directly. This case applies unless the PISP, payer, and ASPSP agree otherwise regarding the collection of additional information for the purposes of providing the PIS.

However, a number of respondents have inquired about the specific type of information included in the data exchange. They needed to know if it includes things like overdraft limits, waiting transactions (those with future execution dates), failed transactions, standing orders and their details, direct debit authorizations, a list of associated payment instruments, and so on. According to the authority's analysis, because ASPSPs have different online platforms for their PSUs, with potentially different information, and because PSD2 does not harmonize the information, the RTS can only require that if the ASPSP provides a dedicated interface, the information be “the same information” as what is available under the customer online interface.

Moreover, when a payment transaction is about to be executed, ASPSPs must immediately confirm to PSPs whether the amount required for this execution is available on the payer's payment account. This confirmation must be as simple as a 'yes' or 'no' response. In the event that unexpected events or errors occur during the process of identification, authentication, or data element exchange, the ASPSP shall send a notification message to the PISP or AISP, as well as the PSP issuing card-based payment instruments, explaining the reason for those unexpected events or errors. Where the ASPSP provides a dedicated interface for SCA & CSC in accordance with Article 28 of the EBA RTS, the interface shall provide for notification messages concerning unexpected events or errors to be communicated to the other PSP participating in the communication session by any PSP that detects the event or error.

ASPSPs must also have appropriate and effective mechanisms in place to prevent access to information other than from designated payment accounts and associated payment transactions, with the user's explicit consent. It should be noted that explicit consent is required in three situations mentioned in three different PSD2 articles (Articles 65, 66, and 67), as previously stated.

Finally, AISPs must be able to access information from designated payment accounts and associated payment transactions held by ASPSPs in order to perform the AIS in either of the following scenarios:

- whenever the PSU actively seeks such information;
- no more than four times in a 24-hour period where the PSU is not actively requesting such information, unless a higher frequency is agreed upon between the AISP and the ASPSP with the PSU's consent [91][92].

Strong Customer Authentication (SCA)

PSD2 seeks to strengthen security in payments and of customers' personalized credentials by mandating SCA or, as it is sometimes referred to: “2 Factor Authentication”, as an integral component of opening up the payments market to TPPs through CSC provided by the third-party interface. SCA undoubtedly played a significant role in the changes and innovative initiatives established by PSD2's new security obligations [83].

SCA, as defined in PSD2 Article 4(30), is a multi-factor authentication based on the use of two or more elements to validate the user or the transaction. These components are categorized as follows [81]:

- Knowledge – something only the user is aware of. A password, PIN, knowledge-based challenge questions, password, and memorized swiping path are all examples of possible knowledge elements. The card details printed on the card are not a valid knowledge element.
- Possession – something that only the user has/ possesses. Possession of a device evidenced by a One Time Password (OTP) or a signature generated by the device, card reader, etc. is one example of a possible possession element. The printed card details do not constitute a valid possession element.
- Inherence – something the user is. Fingerprint scanning, voice recognition, vein recognition, hand and face geometry, retina and iris scanning, keystroke dynamics, heart rate or other body movement pattern identifying that the PSU is the PSU, and the angle at which the device is held are all possible inherence elements. Importantly, data sent via the 3DS communication protocol is not accepted as an inherence factor [22].

These elements are independent in the sense that a breach of one element does not compromise the reliability of the others, and they are designed to protect the confidentiality of the authentication data [81]. In other words, the vulnerability of one authentication factor should not compromise the security of the second. Solutions that combine knowledge and possession factors with weak protection do not typically meet this requirement [80]. For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link between the amount of the transaction and the payee's account to further protect the user by minimizing risks in the event of errors or fraudulent attacks [81].

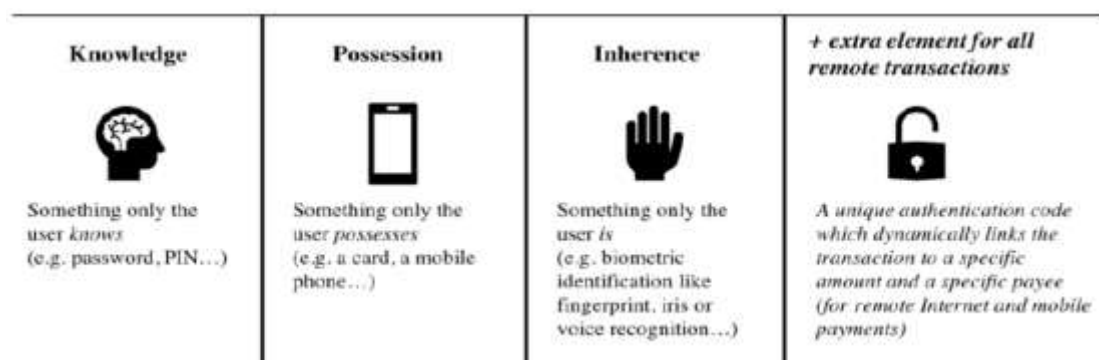


Figure 15. Factors for strong customer authentication [87]

Furthermore, in response to continuing market actors' inquiries about which authentication approaches the EBA considers to be SCA-compliant, and in order to facilitate proper and

timely implementation, the EBA published an opinion on the elements of SCA under the PSD2 on 21 June 2019 [79].

SCA is a key requirement of the EBA GLs because it protects customers from fraud, builds trust in the internet payment ecosystem, and protects sensitive data [80]. Overall, the core principle of SCA is to reduce the risk of fraud and protect the confidentiality of the user's financial and personal data while having as minimal impact on the customer experience as possible, i.e., without introducing too much friction into the payment process [8].

According to Article 97 PSD2 (Authentication), a SCA is required whenever PSUs (individually or through an intermediary) access their payment account online, trigger/initiate an electronic payment process, or engage in an act involving the risk of fraud in payment transactions or other misuse via remote access. The elements “amount” and “payment recipient” must be dynamically incorporated into the data submitted for authentication in the case of a remote payment operation [90]. Authentication refers to procedures that enable a PSP to verify a PSU's identity or the validity of using a specific payment instrument, including the use of user-personalized security details [87].

It is critical to provide a clear analysis referring to the aforementioned three scenarios and the security rules where SCA is required to be applied. More specifically:

1. The PSU (or payer) can access his/her payment account online, for example, via his/her e-banking platform, which can be accessed via a computer/browser or a banking app on his/her mobile device (smartphone, tablet or others). SCA is required in this scenario under Article 97(1)(a), unless the PSU is simply accessing the account balance and/or transaction history for the previous 90 days (Article 10 of the EBA's RTS for SCA & CSC). However, SCA is required as an exception to the exception if (i) the user is accessing the above information for the first time, or (ii) the user has not accessed the above information with SCA in more than 90 days. More information on the SCA exemptions will be examined in the following sections.
2. The payer initiates an electronic payment, whether in a physical store or through an ATM withdrawal, or remotely, e.g., online through a browser on his or her computer or mobile phone, or through an app on his or her mobile phone. The SCA must include “*elements which dynamically link the transaction to a specific amount and a specific payee*” [22]. The payer must also be informed of the amount of the payment transaction and the payee; any changes to these factors must result in the generation of a new authentication code [84]. For example, if SMS (Short Messaging System) is the SCA method used by the payer's PSP, an OTP is sent stating that the payer is attempting to buy from the respective merchant for an amount of, say, 100 EUR. In the context of a card, the authentication code may include cryptograms that represent the transaction's digital signature. This section specifies additional requirements for dynamic linking.

In addition, the application of SCA can be limited to three distinct types of payments. The first is referred to as direct debits, which are generally considered to be initiated by the payee (rather than the payer) and thus are exempt from SCA requirements. The second, which is subject to the SCA principle, is related to credit transfers. They are commonly thought to be initiated by the payer and include e-money transfers. Card payments are the third type of payment, and are generally considered to be initiated by the payer through the payee, and thus are subject to

the SCA requirements. Transactions (MIT) are not subject to SCA requirements, as evidenced by the following response to question 4031 in the EBA Q&A tool: *“where the payer has given a mandate authorising the payee to initiate a transaction or a series of transactions through a particular payment instrument that is issued to be used by the payer to initiate the transactions, and where the mandate is based on an agreement between the payer and that payee for the provision of products or services, the transactions initiated thereafter by the payee on the basis of such a mandate can be qualified as payee initiated transactions, provided that those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee”*.

3. The payer performs any action via a remote channel that may pose a risk of payment fraud or other abuses. The EBA clarified in rationale 13 of the RTS final report on SCA & CSC that *“In relation to payment instruments, and as stated in the CP, the EBA understands that Article 97(1)(b) PSD2 applies to electronic payments initiated by the payer, or by the payer through the payee such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only”*. Direct debits are not subject to the SCA requirements because they are initiated by the payee. However, if the payer *“carries out any action through a remote channel which may imply a risk of payment fraud or other abuse”* (Article 97(1)(c)), an SCA is required. The EBA stated in the aforementioned recital 13 that *“an exception is a transaction where the payer’s consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP”*. In this case, the electronic direct debit mandates will be subject to the SCA provisions because they fall under the purview of PSD2 Article 97(1)(c). It should be noted that payees can collect direct debit electronic mandates without the involvement of a PSP. Because PSD2 only applies to PSPs and not to payees, the SCA requirement does not apply to a mandate collected directly by the payee. However, even if considered initiated by the payee, electronic mandates generally fall under SCA requirements because they represent actions through a remote channel that may imply a risk of payment fraud or other abuses. Moreover, Article 2 of the RTS requires PSPs to have transaction monitoring mechanisms in place to detect unauthorized or fraudulent payment transactions in order to apply and exempt the SCA procedure in accordance with article 97 of PSD2. Finally, in its Opinion on elements of SCA under PSD2, the EBA granted on an exceptional basis and in order to avoid unintended negative consequences for some PSUs that NCAs may decide to collaborate with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time for SCA enforcement. The EBA clarified in its Opinion on the deadline and process for completing the migration to SCA for e-commerce card-based payment transactions that the deadline to migrate to SCA was December 31, 2020. The Opinion also specified the actions that should be taken during the migration period [22].

In accordance with PSD2, the EBA developed, in close collaboration with the ECB, a draft RTS outlining the security requirements of SCA, exemptions from SCA application, and the requirements with which security measures must comply in order to protect the confidentiality and integrity of PSUs' PSC. The requirements that PSPs must meet in order to implement SCA security measures, which will be analyzed in detail in the following sections, are summarized below:

- PSPs must implement transaction monitoring mechanisms to detect unauthorized or fraudulent payment transactions.
- PSPs must implement SCA security measures and conduct their testing, evaluation and periodic documentation in accordance with their audit framework.
- Implementation of SCA authentication based on the use of two or more elements (Two-Factor Authentication) and dynamic linking.
- The PSPs' adoption of risk-mitigation measures.
- Maintaining the confidentiality and integrity of the PSC associated with the PSU [83].

Transaction Monitoring

PSPs must put in place a transaction monitoring mechanism to detect unauthorized or fraudulent payment transactions in order to implement the security measures referred to in SCA. This transaction monitoring mechanism, in particular, should be based on an analysis of payment transactions that take into account elements that are typical of the PSU in the context of a normal use of the PSC by the PSU. The PSPs must ensure that the transaction monitoring mechanisms consider, at a minimum, the following risk-based factors:

- lists of authentication elements that have been compromised or stolen;
- the total value of each payment transaction;
- known fraud scenarios in payment service provision;
- signs of malware infection in any authentication procedure session.

Furthermore, where PSPs exempt the application of the SCA security requirements in accordance with Article 16 “Transaction risk analysis” of the EBA's RTS, they must ensure that the transaction monitoring mechanisms consider, at a minimum, and in real-time, each of the risk-based factors listed below:

- the individual PSU's previous spending patterns;
- the payment transaction history of each PSU of the PSP;
- the payer's and payee's location at the time of the payment transaction, if the PSP provides the access device or software;
- the PSU's abnormal payment patterns in relation to the payment transaction history;
- If the PSP provides the access device or software, a log of the PSU's use of the access device or software, as well as any abnormal use of the access device or software.

Furthermore, electronic payment services must be carried out in a secure manner, using technologies capable of ensuring the safe authentication of the user and reducing the risk of fraud to the greatest extent possible. The authentication procedure must include, in general, transaction monitoring mechanisms to detect attempts to use a PSU's PSC that were lost, stolen, or misappropriated, as well as mechanisms to ensure that the PSU is the legitimate user and thus consenting to the transfer of funds and access to its account information through normal PSC use.

Security Measures Review

Because fraud methods are constantly evolving, the requirements for SCA should allow for innovation in technical solutions to address the emergence of new threats to electronic payment security. To ensure that the requirements of this regulation are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of SCA and its exemptions, the measures to protect the

confidentiality and integrity of the PSCs, and the measures establishing CSC be documented, tested, evaluated, and audited on a regular basis by internal or external independent and qualified auditors. Such a review can be carried out in accordance with the PSP's applicable audit framework.

Also, the interval between audit reviews must be determined in accordance with the relevant accounting and statutory audit framework applicable to the PSP. PSPs that use the Article 16 exemption should conduct an audit of the methodology, model, and reported fraud rates at least once a year. It should also be noted that the audit review will evaluate and report on the PSP's security measures' compliance with the requirements outlined in this regulation. NCAs should have full access to this report upon request.

One-Time Authentication Code

The EBA has established a number of relevant security measures in order for SCA requirements to be met. However, the generation of authentication codes, which play an important role in SCA-compliant transactions, is at the core of these measures. The authentication code is the generation result of one or more factors (knowledge, possession, and inheritance) that are used for SCA process applied by PSPs, as clearly described in the Official Journal of the EU referencing PSD2 legislation, and specifically Article 97(1) of PSD2 [24]. In other words, the authentication code is a password that is generated once the PSP has confirmed the two (or more) elements. According to the FAQ that comes with the PSD2, a possession element for the SCA could be a device that generates the authentication code. The authentication code can only be accepted by the PSP once it has been generated and used by the payer (or PSU) to access its payment account online, initiate an electronic payment transaction, or carry out any action through a remote channel that may imply a risk of payment fraud or other abuses.

Article 4 of the EBA's RTS outlines the conditions that must be met for PSPs to accept authentication codes submitted by payers. To begin, payers must use authentication codes when accessing their online payment accounts, initiating electronic payment transactions, or performing any action via a remote channel that may expose them to online fraud or other digital threats. Furthermore, when accepting authentication codes, PSPs must follow some general rules for authentication codes. Simply put, the conditions are as follows:

- The authentication factors (knowledge, possession, and inheritance) submitted by payers cannot be derived from the disclosure of the authentication code.
- It is not possible to generate a new authentication code based on the knowledge of any previously generated authentication code.
- The authentication code cannot be forged.

Although SCA authentication codes are designed to increase the security of payment transactions, it is important to note that there are some limitations to their use. This contributes to the secure use of these codes and makes them more difficult to exploit. The restrictions listed below ensure the security of the authentication codes to be regulated:

- In scenarios where a code does not follow the aforementioned rules and authentication fails to generate an authentication code, it must be impossible to determine which of the authentication factors submitted was incorrect. In other words, a failure of one of the authentication factors should not imply a failure of any of the others.

- The number of consecutive failed authentication attempts that can occur cannot exceed five in a given period of time; if more than five failed attempts occur, the payer will be temporarily or permanently blocked from their account.
- Where the block is temporary, the duration of the block and the number of retries before applying a permanent block shall be determined based on the characteristics of the service provided to the payer and all relevant risks involved, taking into account, at a minimum, the factors mentioned in Article 2. (3).
- After authenticating for access to one's online payment account, the maximum time without payer activity must not exceed five minutes.
- If a payer is blocked from their account, the payer must be notified before the block is made permanent.
- Where a block has been made permanent, a secure procedure must be established to allow the payer to regain use of the blocked electronic payment instruments.
- In accordance with CSC requirements, communication sessions should be protected against the capture of authentication data transmitted during authentication and manipulation by unauthorized parties.
- The authentication code should not be sent via the same channel that the customer used to start the authentication procedure [92][72].

Taking all of this into account, it is clear that the authentication procedure defined by the bank under PSD2 has opened the door for TPPs to take charge of the process, but only after a specific preventive contractual agreement with the bank. In the same context, the generation of the authentication code is critical to the process. Not only for the aforementioned security reasons, but also to limit the claims of non-arranged information from users directly to a maximum of two accesses per day. Having said that, a new requirement for TPPs is created, which concerns the need for repeated authorization to access data being performed. To be more specific, one of the most significant changes brought about by RTS was the ability for the user to authorize the AISP to question its own checking account. In this context, an AISP could access automatically no more than twice per day and for no more than one month after the last day of SCA. To that end, the requirement suggests that an authentication Token with temporary validity be generated, which, once verified by the ASPSP, allows the AISP to access services without further user interaction.

A possible way to implement this service, which is widely used to authorize access to “protected” contents to external applications, could anticipate the use of the OAuth2.0 framework, which involves the use of a token exchanged through TLS channel ([RFC 6749](#)) to be associated with the correct security principals, providing token encryption, and/or achieving the appropriate security certifications (e.g., PCI-DSS and/or ISO 27001) with regard to the systems in scope. The following repetitive process steps are depicted in the diagram below:

- A. The client begins the authorization process by entering the credentials obtained by the user through the ASPSP's services.
- B. If the credentials are valid, the token and (if applicable) the refresh token are returned.
- C. The client requests service access.
- D. If the token is valid, the Bank returns the requested value.
- E. Points C and D can be repeated indefinitely as long as the token remains valid.
- F. The client re-starts the authorization process using the refresh token obtained in step B. The process begins again at step B [89].

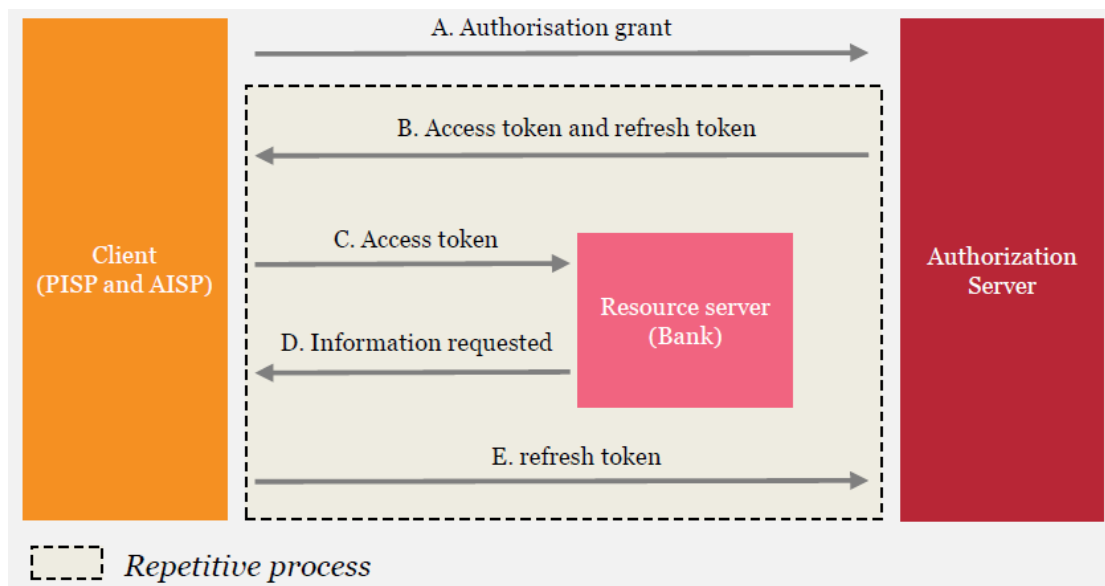


Figure 16. Repetitive authorization to access to data [89]

Dynamic Linking

Because electronic remote payment transactions are more vulnerable to fraud, additional requirements for the SCA of such transactions are required, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction. By imposing this requirement, Articles 97(2) of PSD2 and 5(1) of the RTS strengthen the required authentication.

Dynamic linking is enabled by the generation of authentication codes, which are subject to stringent security requirements. This means that the generated authentication code must be associated with a specific amount and payee. Any modification should render it null and void. This establishes the payment order's “integrity”. The RTS, on the other hand, does not appear to require that third parties, such as banks, be able to verify the authentication or integrity of the payment order. This obligation exists only in the user's relationship with the authenticating PSP. It does not, for example, require that the authentication code be secured by a digital signature or another specific technique that establishes “non-repudiation”. The RTS most likely does not impose this requirement because digital signature technology is not widely used yet, or because it must remain technologically neutral. As a result, as long as the security requirements are met, authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures, or other cryptographically underpinned validity assertions using keys and/or cryptographic material stored in the authentication elements.

Furthermore, the PSP is required to inform the payer of the amount and the payee. The generated authentication code must be specific to the amount of the payment transaction and the payee specified by the payer when initiating the transaction. Finally, the authentication code accepted by the PSP corresponds to the original specific amount of the payment transaction as well as the payee specified by the payer. Any changes to the amount or payee will render the generated authentication code invalid.

Pursuant to RTS Article 5(2), the PSP should implement security measures to ensure the confidentiality, authenticity, and integrity of the amount, payee, and displayed information during all phases of authentication, including the generation, transmission, and use of the

authentication code [86]. For the purposes of these requirements, and where PSPs use SCA in accordance with Article 97(2) of PSD2 in relation to a card-based payment transaction for which the payer has given consent to the exact amount of funds to be blocked in accordance with Article 75(1) of that Directive, the authentication code must be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction. Similarly, when SCA is used in accordance with Article 97(2) of PSD2 for payment transactions in which the payer has given consent to execute a batch of remote electronic payment transactions to one or more payees, the authentication code must be specific to the total amount of the batch of payment transactions as well as to the payees specified [92].

Although Article 5 of the RTS only applies to electronic remote payment transactions, the underlying principles are applicable to AIS as well. In this case, a change in the privileged service provider or the scope of access would render the authentication code invalid. Furthermore, the user must be made aware of the privileged provider and the precise scope of the access throughout all phases of the authentication.

Overall, dynamic linking is important for SCA implementation, not only because it provides additional security guarantees (non-repudiation), but also because signed statements can be passed on by the PSP and verified by the bank itself. Without this requirement, the RTS cannot eliminate the additional risks posed by allowing PSPs to use their own authentication procedures [86].

SCA Elements Requirements

To ensure the application of SCA, adequate security features for the SCA elements must be required. In particular, for elements categorized as knowledge, which are associated with something only the user knows, PSPs must implement measures to reduce the risk that these elements are discovered by, or disclosed to, unauthorized parties. To prevent their disclosure to unauthorized parties, the payer's use of this type of element must also be subject to mitigation measures. Among the recommended measures is the delineation of the length or complexity of the password, the PIN, the passcode, and so on. According to the possession elements (something that only the user possesses), PSPs should also take measures to reduce the risk that these elements will be discovered or disclosed to unauthorized parties, such as defining algorithm specifications, key length, and information entropy. Again, the payer's use of elements classified as possession is subject to measures designed to prevent the elements from being replicated. Finally, for the third category of SCA elements, which refers to devices and software that read inherence elements (something the user is), the mitigation measures that PSPs can apply for the potential risks of being the elements uncovered by unauthorized entities could be algorithm specifications, biometric sensor, or template protection features. At a minimum, the access devices and software must ensure that an unauthorized party cannot be authenticated as the payer. Furthermore, the payer's use of elements classified as inherence should be measured to ensure that the devices and software provide resistance to unauthorized use of the elements through access to the devices and software.

It is also necessary to define security requirements in terms of technology, algorithms, and parameters, ensuring that these elements are independent of one another so that a breach in one does not jeopardize the reliability of the others. When any of these elements or the authentication code are used through a multi-purpose device, such as a tablet or a mobile phone, which can be used for both giving the payment instruction and being used in the

authentication process, PSPs must implement security measures to mitigate the risk of the multi-purpose device being compromised. To that end, the following mitigating measures must be implemented:

- the use of separate secure execution environments via software installed within the multi-purpose device;
- mechanisms to ensure that the software or device has not been altered by the payer or a third-party, or mechanisms to mitigate the consequences of such alteration if it has occurred [92].

In terms of practical implementation, most banks appear likely to rely on the knowledge factor option, such as a PIN, and then choose between possession and inherence as the second factor. The draft RTS raised some questions about the second element, possession. Banks will prioritize possession-based solutions that use a single device to initiate the authentication procedure and receive the authentication code. As a result, banks should consider the technical separation of the different authentication elements within one device when reorganizing their authentication methods. While a possession-focused solution would be technologically strong, regardless of the challenges, it may not provide the level of accuracy required. As a result of this, many banks are looking into inherence to address the second factor of authentication [77].

The EBA Opinion report on SCA elements clarifies the EBA's view on what constitutes or does not constitute each type of element under the implementation of the RTS on SCA and CSC, so that the various payment markets can be facilitated on the security practices they will ultimately decide to pursue. In terms of the inherence element, the Opinion states that *“communication protocols such as EMV® 3-D Secure provide a means for merchants to support the use of SCA. The EBA notes that versions 2.0 and newer support a variety of SCA methods, while trying to ensure customer convenience, limiting fraud through data sharing and transaction risk analysis, and enable the use of exemptions set out in the RTS. For those reasons, the EBA encourages the use of such communication protocols and expedient onboarding. Older protocols such as EMV® 3-D Secure version 1.0, although supporting the use of SCA, are not fully adapted to PSD2. For instance, they do not include the possibility of using exemptions or use all forms of SCA approaches.”* [78]. The most recent version of the 3D-Secure (3DS) protocol allows for new authentication processes such as fingerprint or facial recognition, as well as a much more user-friendly payment process on mobile devices and complements digital wallets such as Apple Pay or Google Pay. It also enables the acquirer to send richer transaction data to the issuer, potentially resulting in higher authentication rates [8].

According to the possession element, and in response to stakeholder inquiries, the EBA believes that card details and card security codes printed on the card cannot constitute a possession element. However, dynamic card security codes (where the code is not printed on the card and changes on a regular basis) may provide evidence of possession in accordance with Article 7 of the RTS. Finally, the EBA believes that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passcode, and a memorized swiping path (as opposed to keystroke dynamics, or how the PSU types or swipes, which could be considered an inherence element) [81].

The three (3) tables below summarize the views expressed in the EBA's Opinion on each SCA element. The EBA stated that these tables are only for illustration purposes, and that

the possible elements included reflect current market practices and developments at the time of the opinion's publication [78].

Element	Compliant with SCA?*
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

Table 1. Non-exhaustive list of possible inherence elements. Source: EBA-Op-2019-06

Element	Compliant with SCA?*
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	Yes
App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device	No
Card with possession evidenced by card details (printed on the card)	No (for approaches currently observed in the market)
Card with possession evidenced by a printed element (such as an OTP list)	No (for approaches currently observed in the market)

*Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.

Table 2. Non-exhaustive list of possible possession elements. Source: EBA-Op-2019-06

Element	Compliant with SCA?*
Password	Yes
PIN	Yes
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	No (for approaches currently observed in the market)
Printed matrix card or OTP list	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

Table 3. Non-exhaustive list of possible knowledge elements. Source: EBA-Op-2019-06

SCA Interface Implementation

The bank's SCA interface should allow PSPs to rely on all of the authentication procedures that the bank provides to the user. This option makes it easier to provide payment services. It enables a PSP to provide services without developing and deploying its own SCA. PSPs can instruct the bank to initiate the authentication procedure in conjunction with the payment order or request for information. Nonetheless, even after the release of the EBA's draft RTS, it remains unclear how this authentication should be resolved and what the authentication technologies should eventually look like. However, the following figures highlight the most significant variations.

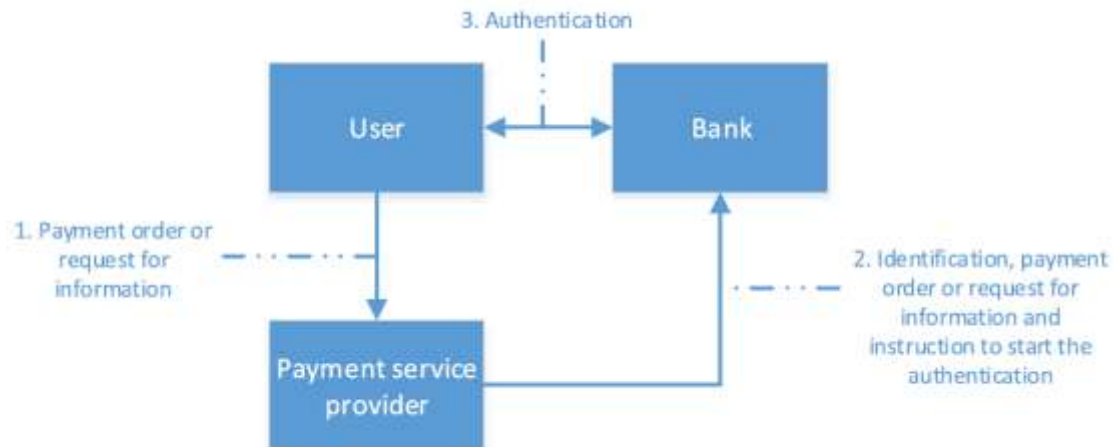


Figure 17. SCA Interface: Redirection or decoupled approach [86]

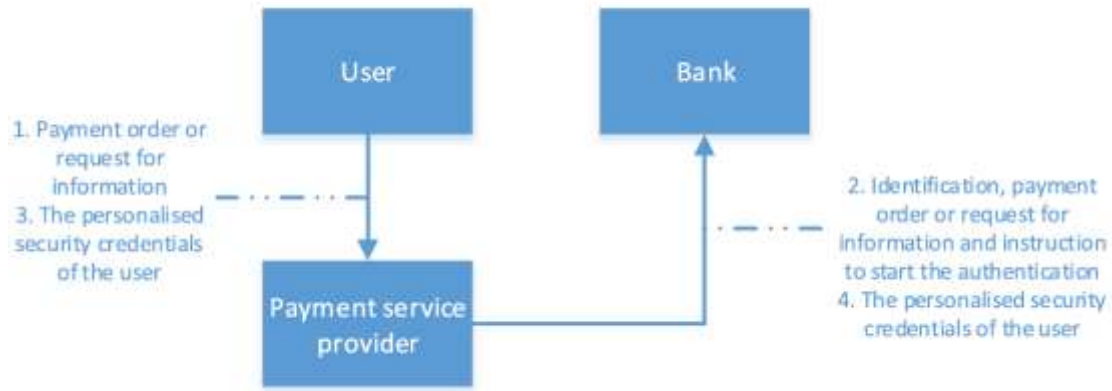


Figure 18. SCA Interface: Embedded approach [86]

According to RTS Article 30(2)(b), the interface should establish and maintain communication sessions between the bank, PSP, and user. The existence of a communication session between the bank and the user implies that the authentication can be resolved without involving the PSP. Instead, the PSP redirects the user to the bank or uses a decoupled approach for authentication. The decoupled interface approach can be based on other technical interfaces in accordance with PSD2 Articles 66 and 67 by using a federation protocol, such as Security Assertion Markup Language (SAML) or OpenID Connect (OIDC), which is based on the OAuth 2.0 Authorization Framework. These standardized, simple, and user-driven authentication protocols and frameworks enable authentication and authorization without revealing the user's PSC to TPPs [90]. As a result, this is consistent with the PSD2 goals. An AISP may not request sensitive payment data, including PSC, and a PISP may not store it. Furthermore, at the time of the authorization application, Article 5(1)(g) of the PSD2 requires a PI to submit a description of the process used to restrict access to sensitive payment data [77].

The system of Figure 17 keeps security risks to a minimum. Potential attackers cannot steal or intercept security credentials from the PSP because the PSP does not have access to them and cannot abuse them. These benefits are lost if the authentication, including the PSC issued by the bank, is handled entirely or partially by the PSP using an embedded approach. This system also makes it easier to commit fraud. Prior to PSD2, banks warned customers not to share their PIN or other security credentials with anyone. These warnings cannot be issued if the PSD2 allows the Figure 18 system. This allows a criminal to impersonate a legitimate PSP in order to induce a user to share his PSC.

Several norms indicate that this system is permissible. Articles 66(3)(b) and 67(2)(b) of the PSD2 state that PSPs must ensure that PSC are not accessible to anyone other than the user and the issuer of the credentials. Furthermore, the articles require them to send security credentials via secure and efficient channels. Following that, Article 30(2) of the RTS states that the interface must ensure the integrity and confidentiality of credentials transmitted by or through PSPs. Finally, in accordance with Article 35(5) of the RTS, PSPs must ensure that transmitted PSC and authentication codes are not readable by any staff at any time. They are required to notify the user and the issuer if the confidentiality of credentials within their sphere of competence is compromised. These standards demonstrate that PSPs can act as an intermediary in an authentication procedure provided by another party, such as a bank [86].

To conclude this section, it is worthwhile to provide a description of the steps that must be taken in the context of the XS2A and authentication process by the parties involved. Figure 19 depicts the “triangular relationship” implied by Article 97(5) PSD2 and Article 27(3)(a) between the PSU (User), the TPP (Service Provider), and the ASPSP (Identity Provider). The procedure is broken down into the following steps:

1. At the TPP, the PSU requests a specific action.
2. The TPP sends an appropriate request to the ASPSP. According to Article 66 PSD2, this may contain transaction information for a payment initiation. Alternatively, the transaction data could be sent to the ASPSP in the following step.
3. The ASPSP redirects the PSU to the authentication endpoint to request permission for a specific transaction.
4. In this step, the PSU is strongly authenticated, and the requested action is authorized.
5. A corresponding response is returned to the TPP following successful user consent, authentication, and transaction authorization.
6. The TPP may now, for example, invoke the business interface corresponding to the use case under consideration at the ASPSP in accordance with Article 66 or 67. In the case of a payment transaction, the response may contain transaction data that is integrity protected and possibly encrypted. Following step, non-transactional interfaces such as account information retrieval may be used (6).
7. Finally, the process is acknowledged by the PSU.

Among the currently relevant international standards that enable strong authentication in the “triangular” relationship depicted in figure 19, the aforementioned SAML Version 2.0 and the OAuth 2.0-based OpenID Connect deserve special mention. While the two protocols differ in technical details, they both support the architecture depicted in Figure 17 and thus could serve as the foundation for the implementation of PSD2-specific interfaces. Thus, it is theoretically possible to specify a corresponding PSD2 interface based on both SAML and OAuth 2.0/ OpenID Connect, with technical interfaces based on both SOAP and REST-based web services [90].

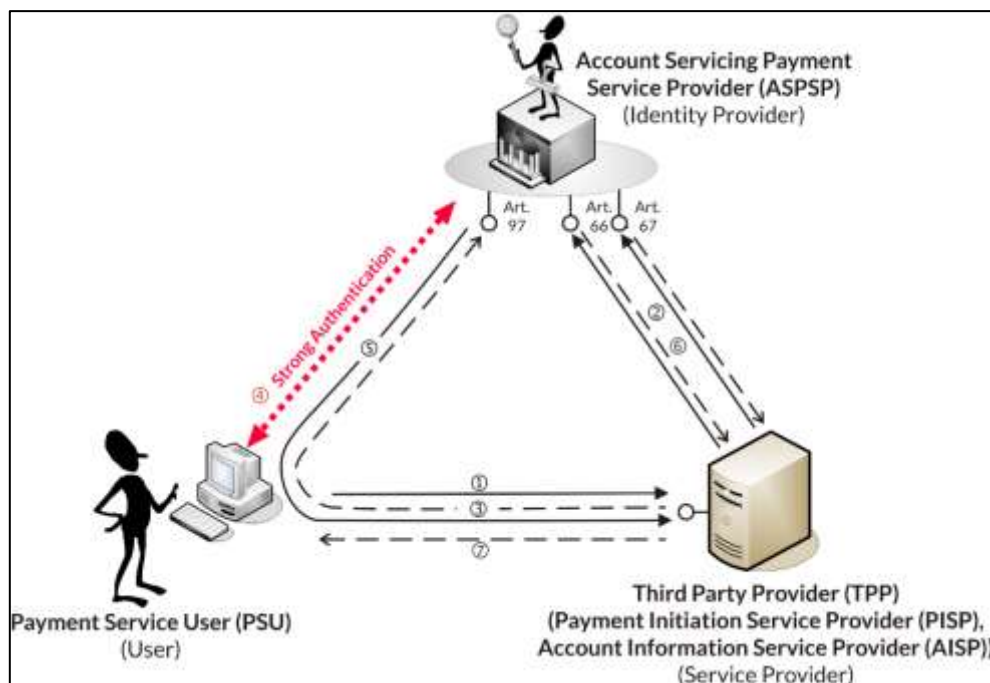


Figure 19. Co-operation between PSU, TPP and ASPSP according to the PSD2 [90]

SCA Exemptions

The PSD2 introduced SCA to make payments more secure by requiring higher levels of authentication when completing a transaction. However, some payments or account access are exempt from the SCA requirement, primarily in the context of internet purchases and “one click” payment experiences [85]. While similar exemptions are available for online banking services, it is unclear whether they improve the user experience or simply increase the complexity of the offering [83].

Exemptions from having to apply SCA under PSD2 are granted based on strict criteria. These are the following:

- the degree of risk associated with the service provided;
- the transaction's amount and/or frequency, and
- the payment channel used to complete the transaction.

PSD2 also introduces a liability shift, with providers who fail to properly authenticate a transaction now held liable for any resulting breaches. If the payer's PSP does not require SCA, the payer will not be held liable for any financial losses unless the payer acted fraudulently. If the payee - or the payee's PSP - fails to accept SCA, the payer's PSP will be required to refund the financial loss [77].

The EBA's RTS on SCA and CSC specifies the cases in which strong authentication measures are not required. Adoption of such measures, in particular, is at the discretion of the institution and is based on conditions related to the following scenarios:

1. Only accessing payment account information

PSPs are exempt from the application of SCA where a PSU is limited to accessing either or both of the following items online without disclosing sensitive payment data, subject to Article 10 (2) of RTS and compliance with the requirements outlined in Article 2 of RTS:

- the balance of one or more payment accounts;
- payment transactions made in the last 90 days using one or more designated payment accounts [92].

2. Contactless payments at point of sale for low value amounts

- Cumulative Limits and Counter Resetting: The following information is important if the card-based or host-based accumulator approaches are used. To be clear, the cumulative limits (EUR 150 or five transactions) apply separately, but the value-based approach (EUR 150) is preferred in order to minimize the impact on cardholder experience. This recommendation reflects the fact that, in markets with high levels of contactless usage, consumers now see contactless as a highly convenient way to make low-value payments, and they frequently make multiple transactions in a day. Contactless transaction fraud rates are also very low, typically less than 2 basis points. Enforcing SCA through PIN entry every five transactions will be disruptive and inconvenient for consumers while providing little benefit in terms of fraud reduction. Issuers can choose which metric to use, and SCA must be used as soon as the chosen metric is reached.

However, current contactless cards are not necessarily personalized with counters that support the cumulative count or amount requirements specified in the SCA

rules. As a result, Visa has developed a contactless specification, VCPS version 2.2.1 (or higher), that will allow Issuers who prefer to solve SCA at the card level to comply with the required cumulative counts and amounts. Similarly, Issuers who wish to manage the SCA rule using a host-based approach must make changes to their authorization systems, and Acquirers must ensure that all terminals comply with TIG version 1.4 [71].

Another source of concern is that meeting these requirements will necessitate either complete reissuance of payment cards in EU or upgrades to POS terminals in EU. This is neither logistically feasible nor desirable in terms of fraud prevention. Furthermore, upgrading all POS terminals would result in significant overhead and disruption for merchants, and widespread card reissuance would disrupt cardholder experience. To that end, a recommendation could be that the requirement should apply, where applicable, to cards issued after the SCA rules enter into force, i.e., 14 September 2019, and that Issuers should have a card replacement program in place to achieve compliance with the regulation over a reasonable time period for existing cards in circulation. Issuers should collaborate with their regulators on a smooth glide path.

- Contactless Payments at Points of Sale where SCA are not available: There are at least two use cases in which contactless payments are made but there is no physical facility for implementing SCA. They are as follows:
 1. Unattended contactless payment terminals that do not require a PIN entry device, such as ticket machines or vending machines. The SCA rules allow for “unattended terminals for transportation fares and parking fees”. This enables PSPs to avoid using SCA on transactions initiated at these terminals.
 2. Card-based payment instruments associated with devices that can accept contactless payments but do not support SCA [71].

3. Unattended payment terminals for the purpose of paying a transport or parking fare

PSPs are exempt from the application of SCA where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport or parking fare, subject to compliance with the requirements outlined in Article 2 of RTS [92].

4. Trusted beneficiaries and recurring transactions

Principles: In the case of trusted beneficiaries’ exemption for card payments, the SCA provisions are followed as follows:

- Only issuers can create/maintain trusted beneficiaries lists on behalf of cardholders and use the trusted beneficiaries exemption, though issuers may outsource or delegate this solution. Issuers, acquirers, and merchants should collaborate to develop risk policies that optimize the use of the Transaction Risk Analysis (TRA) exemption and track its effectiveness in terms of both fraud prevention and card abandonment reduction. Merchants and acquirers should also consider the trade-off between control and liability protection provided by requesting the exemption.

- Only cardholders can add/remove a merchant from a list of trusted beneficiaries, or consent to an Issuer-suggested addition/removal.
- Acquirers cannot use this exemption, and merchants cannot create the list for the SCA exemption.

Issuer Options: Issuers are not required to provide trusted beneficiary capability to their cardholders. Supporting smooth card transactions with known trusted merchants, on the other hand, provides clear benefits to both cardholders and merchants. If an issuer believes a transaction with a listed merchant is at risk of fraud, it may still be subject to SCA.

Merchant Options: While merchants cannot manage trusted beneficiary lists or enroll themselves in a customer's trusted beneficiary list, they can inform their customers about the benefits of using trusted lists and facilitate the enrollment process by:

1. Advising regular customers on how to add the merchant to their trusted beneficiaries list and promoting the benefits to them.
2. Requesting that an issuer serve the trusted beneficiaries enrolment option form via a SCA challenge when a customer completes a transaction with a merchant who has not been added to their list. Merchants can also ask that an issuer apply SCA to a transaction from a customer who has listed them. They should do this if they are concerned about the transaction's risk by submitting it through 3D-Secure [71].

5. Payments to self

PSPs are exempt from the application of SCA where the payer initiates a credit transfer, the payer and the payee are the same natural or legal person, and both payment accounts are held by the same ASPSP, subject to compliance with the requirements outlined in Article 2 of RTS [92].

6. Low value transactions

SCA is not required for remote electronic low-value transactions if the following conditions are met:

- The remote electronic payment transaction amount does not exceed EUR 30; and
- The sum of the payer's previous remote electronic payment transactions initiated since the last SCA application does not exceed EUR 100; or
- The payer's previous remote electronic payment transactions must not have exceeded 5 consecutive electronic payment transactions since the last SCA application.

The limits (EUR 100 or five transactions) apply separately for clarity. Issuers can select which metric to use, and SCA must be activated as soon as the threshold is reached. In practice, because Acquirers typically do not have visibility into cumulative transaction value and volume counts, this exemption will be available only to Issuers [71].

7. Transaction Risk Analysis (TRA)

The TRA exemption exempts certain transactions from SCA if a thorough risk analysis is performed and the PSPs meet specific fraud thresholds. The use of TRA is critical for providing frictionless payment experiences for low-risk transactions. PSPs, in particular,

are exempt from the application of SCA when the payer initiates a remote electronic payment transaction that the PSP identifies as posing a low level of risk in accordance with the TRA referred to in Article 2(1) of RTS. All of the following conditions should be met for this purpose:

- the amount of the electronic payment transaction does not exceed the Exemption Threshold Value (“ETV”) specified in the table below for “remote card-based payments” and “credit transfers”, which correspond to the PSP's fraud rate for such payment services calculated up to a maximum value of EUR 500;

	<i>Reference Fraud Rate (%) for:</i>	
<i>ETV</i>	<i>Remote card-based payments</i>	<i>Credit transfers</i>
<i>EUR 500</i>	<i>0.01</i>	<i>0.005</i>
<i>EUR 250</i>	<i>0.06</i>	<i>0.01</i>
<i>EUR 100</i>	<i>0.13</i>	<i>0.015</i>

Table 4. Fraud thresholds for TRA exemption. Source: Preparing for PSD2 SCA (2018)

- the transaction monitoring mechanisms enable the PSP to conduct a real-time risk analysis of the electronic payment transaction, taking into account, at a minimum, the risk factors listed in Article 2(3) and (4), and combining them in a detailed risk scoring that allows the PSP to assess the level of risk of the payment transaction;
- regardless of the specific arrangements of the transaction monitoring mechanisms, an electronic payment transaction is identified as posing a low level of risk only when the following conditions are met in conjunction with the aforementioned risk analysis:
 - No unusual spending or behavior of the payer has been identified;
 - No unusual data about the payer's device/software access has been discovered;
 - No malware infection has been identified in any session of the authentication procedure;
 - There is no known fraud scenario in the provision of payment services;
 - The payer's location is not unusual;
 - The payee's location is not flagged as high risk.
- for each transaction type referred to in the preceding table, the PSP's overall fraud rate covering both payment transactions authenticated through SCA and executed under any relevant exemption in accordance with Articles 13 to 16 of the RTS shall be equivalent to or lower than the reference fraud rate for the same type of payment transaction in accordance with the preceding table. The overall fraud rate for each type of payment instrument should be calculated as the total value of unauthorized or fraudulent remote transactions, whether funds were recovered or not, divided by the total value of all remote transactions for the same type of payment instrument, whether authenticated with SCA or executed under any relevant exemption pursuant to Articles 13 to 16 on a rolling quarterly basis (90 days);
- the audit review referred to in Article 3 shall evaluate the calculation of the fraud rate and the resulting figures to ensure that they are complete and accurate.

- the PSP's methodology and model, if any, for calculating fraud rates, as well as the fraud rates themselves, must be adequately documented and made fully available to NCAs upon request;
- in accordance with Article 16, the PSP has notified the NCAs of its intention to use the TRA exemption [92].

8. Secure corporate payments

Corporate payments made by business entities using dedicated processes or protocols that are not available to consumers and already provide high levels of fraud protection may be exempt from SCA.

Commercial cards are given to business clients. Lodge Cards, Central Travel Accounts, and Virtual Cards, for example, are not associated with an individual cardholder; they are only used by the company. As a result, because the payment is initiated in a corporate setting, their exposure to fraud is very low. Furthermore, Virtual Cards are inherently secure because they can be deployed with single-use card numbers or tokens, as well as usage restrictions on merchant categories and values.

PSPs may exempt corporate payment processes and protocols that are only available to payers who are not consumers from SCA if the NCAs determine that they meet the PSD2 security requirements. The requirements imposed by national NCAs before a PSP may rely on this exemption may vary across EEA countries.

It should be noted that PSD2 requires PSPs to provide NCAs with regular, updated, and comprehensive assessments of the operational and security risks associated with the payment services they provide, as well as the adequacy of the mitigation measures and control mechanisms put in place to address those risks. NCAs may require PSPs that do not use SCA under the corporate payments exemption to ensure that the processes and protocols are not subject to SCA are specifically included in this assessment.

The SCA requirement applies when a physical corporate card is issued to an individual named employee and that cardholder employee manually initiates a payment. However, if the same card details are embedded and used in a secure corporate purchasing process (e.g., with a corporate appointed Travel Management Company), these transactions are exempt from SCA because the process is akin to a Virtual Card and will be equally secure, and only available for corporate transactions.

All corporate cards are only available to customers with corporate pay and liability. As a result, the relevant corporate entity is always responsible for settling payments made using these products and, in any event, remains liable for settlement [71].

Personalized Security Credentials (PSC) Protection

The protection of the PSC of the PSUs is a significant part of the SCA requirements and Article 97 PSD2, which defines it. These credentials are typically an internet banking password, an authenticate code used to access the bank's mobile app, or any other method of authenticating with a PSP. As a result, in accordance with Article 97, paragraph 3, PSPs must take appropriate security precautions to protect these personalized security features. In other words, they must ensure the confidentiality and integrity of the PSUs' PSC, including authentication codes, throughout all authentication phases, including display, transmission, and storage. According to Article 66 PSD2, the PSU's PSC, with the

exception of the user and the issuer of the credentials, should not be accessible to other parties and should be transmitted by the relevant PSP through safe and efficient channels.

To that end, PSPs should generally comply with the following requirements:

- PSC are masked when displayed and not fully readable when entered by the PSU during authentication;
- PSC in data format, as well as cryptographic materials related to credential encryption, are not saved in plaintext.
- secret cryptographic material is safeguarded against unauthorized disclosure.

In addition to the latter, the process used by the PSPs to encrypt or otherwise render the PSC unreadable must be fully documented. PSPs must also ensure that the processing and routing of security credentials and authentication codes generated in the context of the SCA process takes place in secure environments in accordance with strong and widely recognized industry standards.

PSD2 defines a number of different acceptable actions and rights that can be applied to this type of credential. However, the regulated application of each action is standardized based on specific requirements, which will be discussed further below. These rights are as follows:

- Creation and transmission of credentials
- Association of credentials with the PSU
- Delivery of credentials, authentication devices and software
- Renewal of PSC
- Destruction, deactivation and revocation

According to Article 20 of the EBA's RTS, PSPs must ensure that PSC are created in a secure environment. The risks arising from unauthorized use of the PSC and the authentication devices and software as a result of their loss, theft, or copying prior to delivery to the payer should be appropriately mitigated by the PSPs.

The latter must also ensure that the entity that is securely associated with the credentials, authentication devices, and software is only the PSU. To that end, PSPs must meet the following requirements based on Article 21:

- The association of the PSU's identity with the PSC, authentication devices, and software takes place in secure environments. In particular, the association must take place in environments under the PSP's control, while also taking into account risks associated with devices and underlying components used during the association process that are not under the PSP's control. The PSP's environments include, but are not limited to, his or her premises, the internet environment provided by the PSP or other similar secure websites, and its automated teller machine services.
- The PSU's identity shall be associated with the PSC and with authentication devices or software via a remote channel using strong authentication.

Following the delivery of the security credentials, authentication devices, and software to the PSU, the PSPs must ensure that this action is carried out in a secure manner designed to address the risks associated with their unauthorized use due to loss, theft, or copying. As a result, PSPs must implement at least one of the following measures:

- effective and secure delivery mechanisms that ensure the PSC, authentication devices, and software are delivered to the legitimate PSU associated with the PSP's credentials, authentication devices, and software;
- mechanisms for the PSP to validate the authenticity of authentication software delivered to the PSU via the internet;
- arrangements ensuring that, where PSC is delivered outside the PSP's premises or via a remote channel:
 - When delivered through the same channel, no unauthorized party can obtain more than one feature of the PSC, the authentication devices, or the software.
 - Prior to use, the delivered PSC, authentication devices, or software must be activated.
 - arrangements to ensure that, where the PSC, authentication devices, or software must be activated prior to their first use, the activation takes place in a secure environment in accordance with the association procedures referred to in Article 21.

Regarding the renewal of credentials as defined in Article 23, PSPs must ensure that the procedures for creating, associating, and delivering the PSC and authentication devices as defined in Articles 20, 21, and 22 are followed.

Last but not least, the destruction, deactivation, and revocation of credentials must all meet specific security requirements. PSPs should specifically ensure that they have effective processes in place to implement each of the following security measures:

- the secure destruction, deactivation, or revocation of the PSC, authentication devices, and software;
- where the PSP distributes reusable authentication devices and software, the secure re-use of a device or software is established, documented, and implemented before making it available to another PSU; and
- the deactivation or revocation of PSC-related information stored in the PSP's systems and databases, as well as, where applicable, in public repositories [92].

Security and Operational Risk Management

While many regulated FIs (including PSPs) will have policies, systems, and controls in place to manage operational and security risks, PSD2 solidifies the requirements with EBA guidance. As previously stated, the main requirement of these provisions is the creation and maintenance of a Risk Management Framework document. An updated version of the framework document must be submitted to the PSP's NCA at least once a year. In doing so, the PSP must also comment on the sufficiency of the mitigation and control mechanisms put in place in response to those risks. This will entail some kind of auditing function.

In order to meet these requirements, the EBA issued the GLs mandated by Article 95 of PSD2, subject to the principle of “proportionality”. This means that all PSPs will have to comply with each GL [84]. The level of detail should be proportionate to the size of the PSP as well as the nature, scope, complexity, and riskiness of the specific services that the PSP offers or intends to offer [93].

The final GLs cover a wide range of security topics, including governance, risk assessment, risk control and mitigation, incident monitoring and reporting, sensitive payment data protection, security measure testing, outsourcing, and customer awareness, education, and communication. Other recent requirements include business continuity management,

scenario-based continuity plans, situational awareness, and continuous learning for a PSP's own personnel, partners, and external stakeholders [83].

Governance

To begin, sound internal governance and an internal control framework that establishes clear responsibilities for FIs' staff, including management bodies, can be used to manage and mitigate operational and security risks. When outsourcing or utilizing TPPs, the related GLs also remind FIs to ensure the effectiveness of the risk-mitigation measures defined by their risk management framework. Contracts and service level agreements should specify this. Nonetheless, FIs should monitor and seek assurance of the level of compliance [94].

Operational and security risk management framework

More specifically, PSPs should establish an effective operational and security risk management framework (hereafter “risk management framework”), which should be approved and reviewed at least once a year by the management body and, where appropriate, senior management. This framework should concentrate on security measures to reduce operational and security risks, and it should be fully integrated into the PSP's overall risk management processes. The risk management framework should include the following elements:

- include a comprehensive security policy document, as required by PSD2 Article 5(1)(j);
- be consistent with the PSP's risk tolerance;
- define and assign key roles and responsibilities, as well as the necessary reporting lines for enforcing security measures and managing security and operational risks;
- establish the procedures and systems required to identify, measure, monitor, and manage the range of risks arising from the PSP's payment-related activities and to which the PSP is exposed, including business continuity plans.

Furthermore, PSPs should ensure that the risk management framework is properly documented and that it is kept up to date with documented “lessons learned” during implementation and monitoring. Before making major changes to infrastructure, processes, or procedures, and after each major operational or security incident affecting the security of payment services, PSPs should assess whether changes or improvements to the risk management framework are required.

Risk management and control models

Another security measure required for PSPs is the establishment of three effective lines of defense, or an equivalent internal risk management and control model, to identify and manage operational and security risks. They must ensure that the aforementioned internal control model has adequate authority, independence, resources, and direct reporting lines to the management body and, where applicable, senior management. It is also critical that the security measures outlined in these GLs be audited by auditors who have expertise in IT security and payments and are operationally independent of the PSP. The frequency and focus of such audits should be determined by the corresponding security risks.

Outsourcing

When operational functions of payment services, including IT systems, are outsourced, PSPs must ensure the effectiveness of the security measures outlined in governance GLs. In addition, appropriate and proportionate security objectives, measures, and performance

targets should be included in contracts and service-level agreements with providers to whom PSPs have outsourced such functions. To ensure that these providers are complying with the established security objectives, measures, and performance targets, they should monitor and seek assurance on the acceptable compliance level [93].

Risk Assessment

The management and mitigation of operational and security risks required by FIs must be implemented through an independent and objective control function that is appropriately separated from ICT operations processes and is not responsible for any internal audit, as well as an independent internal audit function. An updated mapping of their business functions, supporting processes, and information assets should be maintained, and they should be classified in terms of criticality based on data confidentiality, integrity, and availability. Based on this, FIs should assess the operational and security risks that affect them and determine what measures are necessary to mitigate the identified risks [94].

Identification of functions, processes and assets

PSPs must first identify, create, and maintain an inventory of their business functions, key roles, and supporting processes in order to map the importance of each function, role, and supporting process, as well as their interdependencies related to operational and security risks. The same requirement applies to the PSPs' organizations' information assets. This entails identifying, establishing, and regularly updating a relevant inventory, which includes ICT systems, their configurations, other infrastructures, and interconnections with other internal and external systems, so that PSPs can manage the assets that support their critical business functions and processes.

Classification of functions, processes and assets

In terms of criticality, these identified business functions, supporting processes, and information assets should be classified appropriately by the PSPs [93]. To determine the criticality of these identified business functions, supporting processes, and information assets, FIs should consider the confidentiality, integrity, and availability requirements. The accountability and responsibility for the information assets should be clearly defined. When performing a risk assessment, FIs are required to review the adequacy of the classification of information assets and relevant documentation. Furthermore, FIs should prioritize the ICT and security risks that impact the identified and classified business functions, supporting processes, and information assets. This risk assessment should be performed and documented on an annual basis, or at shorter intervals if necessary. Such risk assessments should also be performed on any major changes in infrastructure, processes, or procedures affecting business functions, supporting processes, or information assets, and as a result, financial institutions' current risk assessments should be updated [94].

Risk assessments of functions, processes and assets

PSPs must ensure that threats and vulnerabilities are continuously monitored and that risk scenarios affecting their business functions, critical processes, and information assets are reviewed on a regular basis. PSPs should carry out and document risk assessments at least annually or at shorter intervals as determined by the CA, as part of the obligation to conduct and provide NCAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide, as well as the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid out in Article 95(2) of PSD2. Such risk assessments should also be performed prior

to any major change in infrastructure, process, or procedures affecting payment service security. Based on the risk assessments, PSPs should determine whether and to what extent changes to existing security measures, technologies, and procedures or payment services are required. PSPs should also consider the time required to implement the changes as well as the time required to implement appropriate interim security measures to minimize operational or security incidents, fraud, and potential disruptions in the provision of payment services [93].

Protection

PSD2 emphasizes the importance of developing and implementing preventive security measures in response to identified operational and security risks. These safeguards are necessary to ensure an adequate level of security in light of the risks identified. To that end, PSPs must establish and implement a “defense-in-depth” strategy that includes multi-layered controls covering people, processes, and technology, with each layer acting as a safety net for the layers above it. Defense-in-depth should be understood as defining multiple controls that address the same risk, such as the four-eyes principle, two-factor authentication, network segmentation, and multiple firewalls.

Confidentiality, integrity, and availability of PSPs' critical logical and physical assets, resources, and PSUs' sensitive payment data, whether at rest, in transit, or in use, must also be ensured. If the data contains personal information, such measures must be carried out in accordance with Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001.

PSPs should determine whether changes in the existing operational environment influence the existing security measures or necessitate the adoption of additional measures to mitigate the risk involved on an ongoing basis. These modifications should be included in the PSP's formal change management process, which ensures that changes are properly planned, tested, documented, and authorized. Testing should be performed to incorporate scenarios of relevant and known potential attacks based on the security threats observed and the changes made.

Finally, PSPs should follow the principles of segregation of duties and “least privilege” when designing, developing, and providing payment services. PSPs should pay special attention to IT environment segregation, particularly in the development, testing, and production environments [93].

Data and Systems Integrity and Confidentiality

Sensitive Payment Data

The security of sensitive payment data and user personal information becomes critical. As a result, the PSD2 safeguards are also aimed at protecting the user's personal data. PSPs, in particular, should ensure that the collection, routing, processing, storing and/or archiving, and visualization of sensitive payment data of the PSU is adequate, relevant, and limited to what is required for the provision of its payment services [93]. Article 94 of PSD2 establishes the general data protection standard of the relevant legal framework, requiring PSPs to only access, process, and retain personal data required for the provision of payment services with the explicit consent of the PSU. Moreover, all personal data processing under PSD2 must be in accordance with the General Data Protection Regulations (EU) 2016/679 (GDPR) [75]. Recital 89 also specifies that Directive 95/46/EC (Data protection) and its national implementations apply specifically to the processing of personal data for the provision of payment services. This is also stated in article 94(1) of the PSD2 for PISPs.

According to GDPR article 94, these references should be interpreted as references to the GDPR [86]. Both the PSD2 and the GDPR are intended to strengthen data protection by putting the data owner in the center and requiring his consent to capture, store, or process any data. However, there is a chance of an imperfect fit at first. The following are the main pain points concerning personal data protection as a result of the interaction of GDPR and PSD2, of which ASPSPs should be aware [74]:

- AISP's adherence to data protection principles:

According to Article 33(2) PSD2, AISP's are not bound by Article 94 PSD2. However, Article 67 PSD2 explains AISP's obligation to obtain explicit consent from their users before providing AISP's. Despite the fact that it is widely accepted that Article 94 PSD2 will not be applied to AISP's, particularly Article 94(2) PSD2, *"PSPs shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"*, AISP's (as well as PISP's and banks) must still follow all of the GDPR data processing principles. To comply with GDPR data protection requirements, PISP's, AISP's, and banks must also fully implement data protection by design and data protection by default, as well as recent data protection-oriented technology. Thus, whether AISP's are bound by Article 94 PSD2 or excluded from PSD2 for any reason, AISP's are bound by GDPR, which is more detailed and strictly regulated than Article 94 PSD2. In other words, even if PSD2 did not include a data protection provision, TPP's and banks would still be required to access, process, and retain personal data required for the provision of payment services in accordance with GDPR principles and rules. Furthermore, when AISP's are exempted from Article 94 PSD2, there is no meaningful explanation or benefit to be gained. To clarify the situation, the European Data Protection Board (EDPB) acknowledged that obtaining explicit consent is required for AISP's to provide AISP's under PSD2, *"Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISP's. However, Article 67 (2)(a) of the PSD2 still provides for explicit consent for AISP's for the provision of the service"*. Thus, it is accepted, similarly to the approach of the EDPB and the GL's, that explicit consent is directly about providing a contractual service rather than processing users' personal data. As a result, it is preferable for TPP's to use the GDPR's "necessary for the performance of a contract" legal basis for data processing operations [88].
- Individual Rights and data collection:

According to PSD2 Article 94(2), PSP's may only access a user's personal information with that user's express consent in order to provide their services. The PSD2 is more stringent than the GDPR in this regard. A processing is permitted in accordance with Article 6(1)(a) and (b) of the GDPR if the data subject (customer/user/PSU) has consented to it or if it is required for the performance of a contract to which the data subject is a party. Both requirements must be satisfied, according to Article 94(2) of the PSD2. Additionally, it calls for explicit consent (in some circumstances that have previously been discussed in earlier sections). The EDPB claims that this is a contractual condition that differs from the GDPR's definition of (explicit) permission. The GDPR consent is just one of the grounds available and applies to the processing of personal data generally. PSD2's reference to consent relates to payment services. The data subjects must be fully informed of the purposes for which their personal data will be collected, used, processed, and disclosed prior to signing a contract with a PSP. Their personal data will also be utilized in this regard for marketing and sale opportunities. To make it simple for

individuals to understand the implications of open banking and to give informed, meaningful consent, notifications and consent requests must be kept to a single screen or page [74]. This notification need must be fulfilled by stipulations that are clearly identifiable from the rest of the contract's provisions, and consent may be withdrawn at any moment. Article 7 GDPR requires ASPSPs, who are data controllers, to be able to establish that permission was freely provided. These provisions must be explicitly agreed upon by the data subjects. According to Article 94(1), consent is not required for the processing of personal data necessary for the prevention, investigation, and detection of payment fraud [86].

Furthermore, it is important to understand what constitutes “sensitive payment data” under PSD2. The Directive includes a definition of “sensitive payment data”, however this only applies to PSC that could be used to commit fraud and is distinct from the concept of “special categories of personal data” as defined in GDPR Article 9(1). As a result, it makes no difference what types of data will be exchanged with TPPs. However, some data types are more sensitive to privacy than others and may cause more risks for data subjects. In this instance, data subjects should be able to select the specifics of the shared data while providing explicit consent under PSD2. The following information could be retrieved through bank account access: *“names, addresses, social security numbers, credit card numbers, license plate numbers, income/wage, spending categories (preferences and dedicated worth), medical, religious, location, behavioral (events) and social (contacts)”* [88].

- Processing of personal data:

From the ASPSPs' perspective, there is a legal requirement to share the data with the TPP under the rules of PSD2. Other than consent, this gives a valid basis for the processing. Indeed, PSD2 (Articles 66(1) and (4), as well as Article 67(1)) requires ASPSPs to send all necessary data to the AISP or PISP. The legal duty to allow access to payment data and send payment data to TPP also serves as a legitimate ground for processing personal data under GDPR (see GDPR Articles 6(1)(c) and 6(3)(a)).

First, once a TPP obtains access to a PSU's personal data, the TPP assumes its own duties as a controller in the processing of these data. At that point, it must be understood that, under PSD2, both the ASPSP and the TPP are controllers in their own right, and each is responsible for its own processing (but not the processing of the other party). Furthermore, the TPP is a licensed (or registered, in the case of AISP) company, its actions are overseen by the national supervisory authority, it is not chosen by the ASPSPs, and it is a compulsory interlocutor for the ASPSP. As a result, while ASPSPs are responsible for ensuring that the interfaces they provide work, they are not required by PSD2 to verify a TPP's GDPR compliance.

GDPR requires ASPSPs to ensure the security of data flows. PSD2 and the RTS for SC and CSC establish particular standards for ensuring the security of data transfers from ASPSP to TPP (PISPs and AISPs are also required to ensure secure data transfers). As a result, compliance with the RTS requirements, particularly the CSC must be regarded as sufficient for the ASPSP to meet GDPR requirements relating to the security of the transfer, especially given the ASPSP's legal obligation to allow access to the data under PSD2. However, because the RTS refers to both TPPs and ASPSPs as payment entities, both institutions are required to follow the set-out standards. Compliance with PSD2 and the RTS provides a legal foundation for data transfer from ASPSP to PISP or AIS. Compliance with PSD2, and particularly the

RTS, is thus the proper technical measure to protect the transfer and will suffice for GDPR compliance reasons in this context.

PSD2 and GDPR both mandate the minimization of personal data processing. PSD2 not only incorporates data minimization requirements, but also specifically alludes to this obligation under EU privacy law in explanatory notes (e.g., Recital 29) and article 94(2) [22]. TPPs, in particular, are only permitted to access personal data for the purpose(s) expressly requested by users. In other words, PSD2 states that data should not be used for any reason other than providing the service requested by the PSU, and hence additional uses are incompatible. This signifies that “further processing” is subject to limitations. In this case, the user must either consent under Article 6(1) of the GDPR or the processing must be mandated by EU or MS law to which the controller is subject, such as anti-money laundering or terrorist financing laws. When a payment firm depends on consent, it must meet the consent standards and, in particular, demonstrate that the PSU had a genuine option [61].

Because each PI should have access to varied types and amounts of data based on the services they provide, they must closely adhere to all GDPR principles and standards while providing their services, including data minimization and purpose limitation principles. If TPPs can access all bank account data without restriction, this practice will violate GDPR principles and rules, particularly sensitive personal data processing and obtaining explicit consent in cases of automated decision-making, including profiling, which may have legal consequences for users and have a significant impact on them. Furthermore, no provision in PSD2 offers legal justification or exclusions for banks and TPPs to share sensitive personal data and make automated decisions, including profiling. As a result, banks should take technical steps to isolate accounts that may contain sensitive personal data or data used to develop more accurate user profiles from conventional accounts. Banks and TPPs shall also take the necessary precautions to avoid any access that may reveal sensitive personal data about users that is not required for contract fulfilment. Thus, technical solutions that may aid in the separation of data required for contract execution from unneeded and sensitive personal data should be implemented [88].

For PIS, the GDPR's data minimization criteria are consistent with PSD2's: only data required to initiate a payment transaction may be requested and accessed. This regulation must be followed, particularly when seeking access as indicated in the RTS on SCA (articles 33(4) and 33(5)) and the EBA's Opinion of 13 June 2018 (paragraph 26). For AIS, PSD2 states that the provider shall “*not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules*”. Data minimization criteria will be supported by dedicated interfaces designed to allow TPPs to request certain data sets in accordance with PSD2 rules. It should also be noted that other legal responsibilities than those provided by the PSD2 may apply. This is an example of a duty regarding data content in payment orders.

Furthermore, in the context of AIS and PIS, the TPP offering these services bears main responsibility for information provision to users. PSD2 creates standardized GLs to ensure that TPPs furnish PSUs with required, adequate, and understandable information. Articles 44 and 45 state that, in the interest of efficiency, the required information shall be reasonably proportionate to the needs of the user and delivered in a standard format. The transfer of data from the ASPSP to the TPP could be termed “further processing” by the ASPSP. However, when expressing its approval to the TPP, the PSU should have received information on the data transfer. As a

result, the ASPSP would be excused from explaining this a second time under GDPR Article 13(4). However, ASPSPs may mention in their privacy notices that a possible transfer to an AIS or PISP may occur (because to a legal obligation) [22].

- Data storage and disposal

GDPR requires that data be securely stored and that after any legal, contractual, or regulatory retention limit has elapsed, the data be erased or de-identified. The security safeguards used must be proportionate to the sensitivity of the data. Furthermore, GDPR grants an individual the right to be forgotten and, in certain circumstances, the right to be erased. However, due to the legal complexities involved, these rights are beyond the reach of an open banking framework. PSD2 open banking will broaden traditional banking data flows by putting the client at the center and giving them control over their financial data, including personal information [74].

Systems

In terms of information system security, PSPs should ensure that the software used to provide payment services, including the users' payment-related software, is up to date and that critical security patches are deployed on a regular basis. PSPs should put in place integrity-checking mechanisms to ensure the integrity of their payment services' software, firmware, and information [93].

Access Control

FIs should define, document, and implement logical access control procedures (identity and access management). These procedures should be implemented, enforced, monitored, and reviewed on a regular basis. Controls for monitoring anomalies should also be included. The following elements, where “user” includes technical users, should be implemented at a minimum:

- Only authorized individuals should have physical and logical access to ICT systems. Authorization should be assigned in accordance with the tasks and responsibilities of the staff, and should be limited to individuals who have been properly trained and monitored. PSPs should implement controls to reliably limit such access to ICT systems to those with a legitimate business need. Electronic access to data and systems by applications should be limited to the minimum required to provide the relevant service.
- The operation of access control products, tools, and procedures should prevent access control processes from being compromised or circumvented. Enrollment, delivery, revocation, and withdrawal of corresponding products, tools, and procedures are all included.
- FIs should manage access rights to information assets and supporting systems on a “need-to-know” basis, including for remote access. Users should be granted only those access rights that are strictly necessary to carry out their duties (principle of “least privilege”), i.e., to prevent unjustified access to a large set of data or the allocation of combinations of access rights that could be used to circumvent controls (principle of “segregation of duties”). Access rights should be reviewed on a regular basis.
- The use of generic and shared user accounts should be limited as much as possible, and users should be able to be identified for actions performed in ICT systems.
- FIs should implement strong controls over privileged system access by strictly limiting and closely monitoring accounts with elevated system access entitlements (e.g., administrator accounts). Controls such as roles-based access, logging and

reviewing privileged users' system activities, strong authentication, and anomaly monitoring should be implemented. Remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used to ensure secure communication and reduce risk.

- At the very least, all privileged user activities should be logged and monitored. In accordance with the “risk assessment” security measure, access logs should be secured to prevent unauthorized modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes, and information assets, without prejudice to the retention requirements set out in EU and national law. This information should be used by a financial institution to aid in the identification and investigation of suspicious activities detected during the provision of services.
- Access rights should be granted, withdrawn, or modified as soon as possible, in accordance with predefined approval workflows that include the business owner of the information being accessed (information asset owner). When an employee's employment is terminated, access rights should be revoked as soon as possible.
- Access rights should be reviewed on a regular basis to ensure that users do not have excessive privileges and that access rights are withdrawn when no longer needed.
- FIs should enforce authentication methods that are sufficiently robust to ensure that access control policies and procedures are followed. Authentication methods should be proportionate to the importance of the ICT systems, information, or process being accessed. Based on the relevant risk, this should include at a minimum complex passwords or stronger authentication methods (such as two-factor authentication) [93][94].

Physical Security

PSPs should have adequate physical security measures in place, particularly to protect PSUs' sensitive payment data as well as the ICT systems used to provide payment services. To protect the FIs' premises, data centers, and sensitive areas from unauthorized access and environmental hazards, appropriate measures should be defined, documented, and implemented. Physical access to ICT systems, in particular, should be limited to individuals who have been appropriately trained and monitored, and the authorization should be assigned in accordance with the individual's tasks and responsibilities. This access should also be reviewed on a regular basis to ensure that unnecessary access rights are promptly revoked when they are no longer required. Finally, adequate environmental measures should be proportionate to the importance of the buildings and the criticality of the operations or ICT systems located in these buildings [94].

Detection

Incident Monitoring and Reporting

While PSPs were already required to monitor and report incidents on electronic payments under PSD1, they may find that the requirements under PSD2, as set out in the EBA Revised GLs ([EBA/GL/2021/03](#)), introduce thresholds for incidents that must be reported and make reporting requirements more comprehensive. They are applicable to all payments, not just internet payments. PSPs only need to focus on GLs 1 to 4 (GLs 5 to 8 address the NCAs of MSs). As shown in the figure below, these define what constitutes a major incident, the notification process, delegated and consolidated reporting, and PSP operational and security policies.



Figure 20. Content of the Guidelines on major incident reporting under PSD2 [83]

The GLs, when combined with the requirements of the GDPR and the NIS Directive, have the effect of requiring a plethora of notifications related to the same incident to be sent without undue delay to various authorities at both national and European levels, using different formats based on different criteria. To that end, the guidance provided to PSPs should cover the following areas:

1. Classification as a major incident

The first area outlines a methodology that PSPs must use to clearly differentiate between incidents. This is based on predefined criteria and threshold values, and it allows PSPs to determine which incidents need to be reported. In other words, as outlined in the “Definitions” section of these GLs, PSPs should define these parameters for classifying an event as an operational or security incident. Following that, they must implement early warning indicators that will serve as an alert to the PSP, allowing for the early detection of operational or security incidents [93].

When an incident meets one or more criteria at the “Higher impact level” or three or more criteria at the “Lower impact level”, it is classified as a major incident. If they discover that the threshold has been lowered, they must now report incidents that they were previously not required to report. [83]. The transaction affected, the PSUs affected, the service downtime, the breach of security of network or information systems, the economic impact, the high level of internal escalation, if other PSPs or relevant infrastructures are potentially affected, and the reputational impact are the classification criteria. The “impact level” is “higher” or “lower” depending on the values assigned to thresholds for each of the aforementioned criteria. Additional information is available in the relevant table stated in the EBA GLs.

2. Notification process

After classifying an incident as major, the PSP must gather all relevant information, create a report using a pre-defined template, and submit it to the NCA in the home MS. The report must be provided to the NCA throughout the incident's lifetime for initial, intermediate, and final reports within the specified time frame. For example, after a major incident is

detected, the initial report should be submitted to the NCA within four hours, the interim report within three working days, and the final report within two weeks [83]. The procedure for notifying NCAs outlined in paragraph 3.2 of the GLs overlaps with the Procedure of the EBA GLs on the security of internet payments. The EBA clarified in its “Opinion on the Transition from PSD1 to PSD2” that the Procedure in the major incident reporting GLs supersedes the application of the 2014 GLs on internet payment security [22].

3. Delegated and consolidated reporting

PSPs who wish to delegate reporting obligations under PSD2 to a third-party should notify the NCA in their home MS and ensure that all necessary specific conditions are met. PSPs who wish to allow the designated TPP to fulfill the reporting obligations in a consolidated manner (i.e., by presenting a single report referring to multiple PSPs affected by the same major operational or security incident) should notify the NCA in the home MS, provide the contact information included under “Affected PSP” in the template, and ensure conditions are met. It should be noted that PSPs should not delegate their reporting obligations before informing the NCA in the home MS or after being notified that the outsourcing agreement does not meet the necessary GLs requirements. In the event of delegation, the withdrawal of PSPs' reporting obligations should be communicated to the NCA in the home MS, in accordance with the latter's deadlines and procedures. Any material development affecting the designated TPP and its ability to meet reporting obligations should be reported to the NCA in the home MS by PSPs.

According to Article 96 of PSD2 and these GLs, whenever the designated third party fails to notify the NCA in the home MS of a major operational or security incident, PSPs must materially fulfill their reporting obligations without relying on external assistance. An incident must not be reported twice, once by the PSP and once by the TPP. Finally, when an incident is caused by a disruption in a technical service provider's (or an infrastructure's) service that affects multiple PSPs, the delegated reporting refers to the PSP's individual data (except in the case of consolidated reporting) [77].

4. Operational and security policy

PSPs should ensure that their general operational and security policy clearly defines all incident reporting responsibilities under PSD2, as well as the processes implemented to meet the requirements defined in the current GLs. Appropriate processes and organizational structures should be put in place to ensure consistent and integrated monitoring, handling, and follow-up on operational or security threats that could materially impair their ability to provide payment services [93] [76].

Fraud Detection

As banks implement APIs and open their infrastructure to TPPs under PSD2, fraudsters will have a plethora of new opportunities – at a time when banks have already lost significant amounts to fraud and are engaged in an arms race to stay ahead of ever more sophisticated cyber-criminals [77]. To that end, the EBA, in close collaboration with the ECB, has developed fraud reporting GLs under PSD2 with the goal of ensuring that comparable and reliable data on fraud are collected in all MSs ([EBA/GL/2018/05](#)). GLs require organizations to have solid and detailed reporting structures in place for all payment transactions, not just fraudulent ones, so compliance may necessitate significant upgrade work depending on organizations' current systems and processes [83].

More specifically, FIs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes, and information assets in order to detect anomalous activities in payment service provision. PSPs should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion, as well as breaches of confidentiality, integrity, and availability of information assets used in the provision of payment services, as part of this continuous monitoring. The processes of continuous monitoring and detection should include:

- internal and external factors relevant to business and ICT administrative functions
- transactions to detect unauthorized access by third parties or other entities, as well as internal unauthorized access;
- internal and external threats that could occur.

Furthermore, FIs should develop and implement processes and organizational structures to identify and continuously monitor security threats that could materially impair their ability to provide services. They must actively monitor technological developments in order to be aware of security risks. Detective measures must be implemented, for example, to identify potential information leaks, malicious code and other security threats, and publicly known vulnerabilities in software and hardware, as well as to check for new security updates. The security monitoring process should also assist a FI in understanding the nature of operational or security incidents, identifying trends, and assisting the organization's investigations [93][94].

Business Continuity Management

Article 89 defines PSPs' liability in case they fail to execute payment transactions correctly and on time. This section emphasizes the significance of a solid business continuity policy and plan [7]. Specifically, as stated in paragraph 2 of this article and Title VI of the EBA GLs on internal governance ([EBA/GL/2017/11](#)), FIs should establish a solid business continuity management (BCM) process to maximize their ability to provide services on an ongoing basis and to limit losses in the event of severe business disruption. The relevant internal and external stakeholders are expected to apply BCM by developing response and recovery plans, including testing and subsequent updating based on test results, and having effective crisis communication measures in place so that they can be informed in a timely manner [94].

Business Impact Analysis

To begin, in order to establish sound BCM, PSPs should carefully analyze their exposure to severe business disruptions and assess, quantitatively and qualitatively, their potential impact, using internal and/or external data and scenario analysis. In other words, a business impact analysis (BIA) should be performed. PSPs should prioritize business continuity actions using a risk-based approach based on the identified and classified critical functions, processes, systems, transactions, and interdependencies in accordance with the Risk Assessment GL. Depending on the PSP's business model, this could, for example, facilitate the processing of critical transactions while remediation efforts continue.

In addition, a PSP must implement:

- business continuity plans (BCPs) to ensure that it can respond appropriately to emergencies and continue critical business operations; and

- mitigation measures to be implemented in the event that its payment services and existing contracts are terminated, in order to avoid negative effects on payment systems and PSUs and to ensure the execution of pending payment transactions.
- ICT systems and services that are designed and aligned with their BIA, such as redundancy of certain critical components to prevent disruptions caused by events affecting those components [93].

Scenario-based Business Continuity Planning

Based on the BIAs mentioned above, FIs should develop business continuity plans that are documented and approved by their management bodies. The plans should specifically address risks that could have a negative impact on ICT systems and services. The plans should support goals to safeguard and, if necessary, restore the confidentiality, integrity, and availability of their business functions, supporting processes, and information assets. During the development of these plans, FIs should consult with relevant internal and external stakeholders as needed.

The BCPs that will be implemented should enable FIs to respond appropriately to potential failure scenarios and to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In the event of a severe business disruption that necessitates the implementation of specific business continuity plans, FIs should prioritize business continuity actions using a risk-based approach, which can be based on the risk assessments performed under the “Risk Assessment” section. For PSPs, this may entail, for example, facilitating the continuation of critical transactions while remediation efforts are ongoing.

PSPs should also consider a variety of different scenarios in their BCP, including extreme but plausible ones, to which they may be exposed, such as a cyber-attack scenario, and assess the potential impact of such scenarios. Based on these scenarios, a FI should describe how ICT system and service continuity, as well as the FI's information security, are ensured. In addition, based on the BCM analysis and plausible scenarios identified, the PSP should develop response and recovery plans that include:

- concentrate on the impact on critical functions, processes, systems, transactions, and interdependencies;
- be documented and made available to business and support units, as well as easily accessible in the event of an emergency; and
- be updated in response to test results, new risks and threats identified, and altered recovery objectives and priorities.

Testing of Business Continuity Plans

It is critical that the PSPs put in place BCPs that are tested on a regular basis. PSPs, in particular, should ensure that the critical functions, processes, systems, transactions, and interdependencies are tested at least once a year. The plans should help to protect and, if necessary, restore the integrity and availability of their operations, as well as the confidentiality of their information assets.

Plans should be updated at least once a year, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, changing recovery objectives, and analysis of operationally and technically plausible scenarios that

have not yet occurred, as well as changes in systems and processes, if applicable. During the development of their BCPs, PSPs should consult and coordinate with relevant internal and external stakeholders.

The testing of FIs' BCPs should demonstrate that they can keep their businesses running until critical operations are restored. They should, in particular:

- include testing of a sufficient number of severe but plausible scenarios, including those considered in the development of the BCPs (as well as testing of services provided by third parties, where applicable); This should include transferring critical business functions, supporting processes, and information assets to a disaster recovery environment and demonstrating that they can be run in this manner for a sufficiently representative period of time and that normal operations can be resumed afterwards.
- be designed to challenge the assumptions underlying BCPs, such as governance arrangements and crisis communication plans; and
- include procedures to validate their staff's and processes' ability to respond adequately to the scenarios outlined above.

Finally, it is important to implement a regular monitoring of the effectiveness of their BCPs, as well as documenting and analyzing any challenges or failures that arise from the tests.

Crisis Communications

In the event of a disruption or emergency, as well as during the implementation of the BCPs, financial institutions should ensure that effective crisis communication measures are in place to ensure that all relevant internal and external stakeholders, including NCAs when required by national regulations, and relevant providers (outsourcing providers, group entities, or TPPs), are informed in a timely and appropriate manner.

Testing of Security Measures

The FIs must also perform a variety of information security reviews, assessments, and testing to ensure the effective identification of vulnerabilities in their ICT systems and services. Financial institutions, for example, may conduct gap analysis against information security standards, compliance reviews, internal and external audits of information systems, or physical security audits. Furthermore, good practices such as source code reviews, vulnerability assessments, penetration tests, and red team exercises should be considered by the institution.

In addition, a testing framework for validating the robustness and effectiveness of security measures must be established and implemented. As a result, new threats and vulnerabilities discovered through risk-monitoring activities could be taken into account by the framework.

The testing framework should also include security measures for I payment terminals and devices used for payment service provision, (ii) payment terminals and devices used for PSU authentication, and (iii) devices and software provided by the PSP to the PSU to generate/receive an authentication code. It should also ensure that the following tests are carried out:

- are carried out as part of the formal change management process of the PSP to ensure their robustness and effectiveness;
- are performed by independent testers who have sufficient knowledge, skills, and expertise in testing payment security measures and are not involved in the

- development of the security measures for the corresponding payment services or systems to be tested, at least for final tests prior to putting security measures into operation; and
- include vulnerability scans and penetration tests (including threat-led penetration testing as needed and appropriate) proportionate to the level of risk identified with the business processes and systems.

Furthermore, stakeholders should conduct ongoing and repeated tests of their payment services' security measures. These tests must be performed at least once a year for systems that are critical to the provision of payment services. Non-critical systems, on the other hand, should be tested on a risk-based basis at least every three years. Security measures should be implemented in the event of changes to infrastructure, processes, or procedures, and if changes are made due to major operational or security incidents, or the release of new or significantly changed internet-facing critical applications. The results of the tests should be monitored and evaluated by the PSPs, and security measures should be updated accordingly and without undue delay in the case of critical systems.

Last but not least, testing is required to incorporate scenarios of relevant and known potential attacks based on the security threats observed and the changes made [93][94].

Situational Awareness and Continuous Learning

Another significant security measure introduced by the PSD2 is the training programs that must be completed by the FI's staff. In particular, FIs should establish a training program for all staff and contractors, including periodic security awareness programs, to ensure that they are trained to perform their duties and responsibilities in accordance with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse, or loss, as well as how to address information security-related risks. The training program should ensure that all employees and contractors receive training at least once a year, and more frequently if necessary [94]. Employees in key roles identified in the risk assessment requirement must receive targeted information security training on an annual basis, or more frequently if necessary.

PSPs must develop and implement processes and organizational structures to identify and continuously monitor security and operational threats that could jeopardize their ability to provide payment services. Periodic security awareness programs must be implemented so that PSPs can educate their personnel and address information security risks. These programs should make it mandatory for PSP personnel to report any unusual activity or incidents. Operational or security incidents that have been identified or occurred within and/or outside the organization should also be investigated. Furthermore, key lessons learned from these analyses must be considered, and security measures must be updated accordingly. PSPs should also actively monitor technological developments to stay abreast of security threats [93][94].

Payment Service User Relationship Management

The final security measure is only applicable to PSPs. It specifies requirements for PSU relationship management, such as allowing PSUs to disable specific payment functionalities (where product functionality allows), receiving alerts on initiated and/or failed payment transaction attempts, and assisting PSUs with questions and requests for support. The EBA emphasizes the importance of transparency, so that PSUs are always aware of which PSP is in charge of providing them with payment services [94].

More specifically, PSPs must establish and implement processes to raise PSUs' awareness of security risks associated with payment services by assisting and guiding PSUs. As new threats and vulnerabilities emerge, the assistance and guidance provided to PSUs should be updated, and any changes should be communicated to the PSU. PSPs should allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU where product functionality allows.

Where a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments in accordance with Article 68(1) of PSD2, the PSP should give the payer the option to adjust these limits up to the maximum agreed limit. PSUs must be able to receive alerts on initiated and/or failed payment transaction attempts, allowing them to detect fraudulent or malicious use of their accounts. They should also be kept up to date on changes in security procedures that affect their ability to provide payment services. Finally, PSPs should assist PSUs with all questions, requests for support, and notifications of anomalies or issues relating to payment services security. PSUs should be properly informed about how to obtain such assistance [93].

Mapping Table: PSD2 – ISO/IEC 27001:2022 – PCI DSS

After analyzing and concluding on PSD2 security measures, it is now necessary to exhibit this analysis in a table that will present all key security domains with their related subdomains for the reader's better understanding. However, in order for the various FIs to ensure full and effective PSD2 compliance, a high-level mapping and comparison between the security areas covered by the Directive and those covered by internationally recognized and directly related Standards, PCI DSS and ISO/IEC 27001:2022, was deemed necessary. As a result, stakeholders will have access to a useful resource for understanding how to align security efforts to accomplish PSD2 objectives through the application of these two Standards.

To begin, the PCI DSS (Payment Card Industry Data Security Standard) is a security standard developed by the PCI SSC (PCI Security Standards Council) for industries and processors that take credit or debit card payments. It is founded on the agreement of five global payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. – to include PCI DSS as a technical requirement for compliance with each of their data security procedures [67]. PCI DSS is designed to address the particular security threats and risks that exist in the payments industry. It specifies security criteria for the protection of payment card and sensitive authentication data wherever it is processed, stored, or transferred, as well as validation methods and recommendations to assist companies in understanding the requirements' objective. PCI SSC (Payment Card Industry Security Standards Council) collaborates with merchants, service providers, FIs, technology suppliers, and others in the payments industry, as well as our assessor and forensic investigator communities. This keeps all stakeholders informed of current payment data security concerns and ensures that PCI Standards continue to address such threats [39].

ISO/IEC 27001, on the other hand, is the world's most well-known standard for information security management systems (ISMS). It has been designed to offer requirements for the establishment, implementation, maintenance, and continuous improvement of an ISMS. The adoption of an ISMS is a strategic decision for an organization, and its development and implementation are influenced by the organization's needs and objectives, security requirements, organizational procedures used, and the organization's size and structure. The

ISMS protects the confidentiality, integrity, and availability of information through the use of a risk management process, giving interested parties confidence that risks are adequately managed. Because the ISO/IEC 27001 Standard is broadly focused on ISMS implementation, fulfilling the specified aims implicitly involves assurance that payment data is likewise protected [35].

PCI DSS and the ISO/IEC 27001 Standard are both strong security approaches that address shared security aims and principles as they apply to unique risks. While the ISO/IEC 27001 Standard specifies generic security goals and activities, the PCI DSS provides specific instruction and guidance on how to satisfy payment environment security outcomes. Because PCI DSS and ISO/IEC 27001 are designed for different audiences and purposes, they are not interchangeable, and neither is a replacement for the other.

This mapping is based on the latest version v4.0 of PCI DSS, and the ISO/IEC 27001, using the new version of the Standard published on October 25, 2022. The mapping table below compares each control of the two Standards to the PSD2 standards, as well as identifies and maps the applicable PSD2 requirements for each control. The resulting mapping indicates which security controls contribute to PSD2 compliance and which contribute to PCI DSS compliance. The mapping covers eight (8) domains of the PSD2 security measures discussed above, including some subcategories where applicable, and demonstrates how satisfying them may assist companies in demonstrating how the Standards controls are achieved for payment environments. This mapping can be used by stakeholders to discover potential for control efficiency and greater alignment with organizational security objectives as specified by PSD2. For example, the mapping can assist in determining where the installation of a specific security control from PCI DSS or ISO/IEC 27001 can satisfy a PSD2 need, or else a table subdomain to be applied. Furthermore, these Standards may assist an entity in being better prepared for internal assessments performed in its organization to determine the effectiveness of PSD2 security measures employed. However, PCI DSS and ISO/IEC 27001 may not guarantee that the Standards' implementation will cover all areas of PSD2 security requirements. As a result, the following high-level mapping allows a consistent and coordinated approach relevant to the implementation degree of the individual Standards for a financial organization's best possible compliance with PSD2 security criteria. Furthermore, it should be emphasized that this mapping table is not a guidance for showing full PSD2 compliance, nor does meeting a PSD2 requirement through ISO/IEC 27001 imply meeting the same need through PCI DSS [39].

	PSD2	PCI DSS v4.0	ISO/IEC 27001:2022
Strong Customer Authentication	Strong Customer Authentication (SCA)	Requirement 8 (8.2, 8.3): Identify and authenticate access to system components	A.5.14 Information transfer A.5.15 Access control A.5.16 Identity Management A.5.17 Authentication information A.8.5 Secure authentication

	Personalized Security Credentials Protection	Requirement 2 (2.3, 2.6): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (all): Protect stored cardholder data Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 8 (8.1, 8.2, 8.3, 8.5, 8.6, 8.7): Identify and authenticate access to system components	A.5.14 Information transfer A.5.15 Access control A.5.16 Identity management A.5.17 Authentication information A.5.18 Access rights A.5.34 Privacy and protection of PII A.8.2 Privileged access rights A.8.3 Information access restriction A.8.5 Secure authentication A.8.26 Application security requirements A.8.24 Use of Cryptography ISO 27701:2019 - Clause 6.15.1.4 Privacy and protection of personally identifiable information ISO 27701:2019 - Clause 7.2 Conditions for collection and processing ISO 27701:2019 - Clause 7.3 Obligations to PII principals ISO 27701:2019 - Clause 7.5 PII sharing, transfer and disclosure ISO 27701:2019 - Clause 8.2 Conditions for collection and processing
	Open Banking API Standardization	Requirement 2 (2.2, 2.3): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 4: Encrypt transmission of cardholder data across open, public networks Requirement 6: Develop and maintain secure systems and applications	A.5.1 Policies for information security A.5.14 Information transfer A.5.16 Identity Management A.5.17 Authentication information A.5.37 Documented operating procedures A.8 Technological Controls
	TPP User Management	Requirement 7 (7.2): Restrict access to cardholder data by business need-to-know Requirement 8 (8.1, 8.2, 8.6): Identify and authenticate access to system components	A.5.15 Access Control A.5.16 Identity Management A.5.17 Authentication information A.8.3 Information access restriction A.8.24 Use of Cryptography
	Secure Communication Session	Requirement 2 (2.3, 2.6): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 6 (all): Develop and maintain secure systems and applications	A.5.14 Information transfer A.8.24 Use of Cryptography A.8.26 Application Security Requirements
	Data Exchanges	Requirement 3 (3.1, 3.2): Protect stored cardholder data Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 8 (8.7): Identify and authenticate access to system components Requirement 10 (all): Track and monitor all access to network resources and cardholder data Requirement 11 (11.5): Regularly test security systems and processes Requirement 12 (12.8, 12.9): Maintain a policy that addresses information security for all personnel	A.5.14 Information transfer A.5.31 Legal, statutory, regulatory and contractual requirements A.6.8 Information security event reporting A.8.3 Information access restriction A.8.12 Data leakage prevention A.8.15 Logging A.8.16 Monitoring activities

Governance	Governance	Requirement 1 (1.5): Install and maintain a firewall configuration to protect cardholder data Requirement 2 (2.2, 2.5): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (3.7): Protect stored cardholder data Requirement 4 (4.3): Encrypt transmission of cardholder data across open, public networks Requirement 5 (5.4): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.7): Develop and maintain secure systems and applications Requirement 7 (7.3): Restrict access to cardholder data by business need-to-know Requirement 8 (8.1, 8.8): Identify and authenticate access to system components Requirement 9 (9.10): Restrict physical access to cardholder data Requirement 10 (10.8, 10.9): Track and monitor all access to network resources and cardholder data Requirement 11 (11.6): Regularly test security systems and processes Requirement 12 (all): Maintain a policy that addresses information security for all personnel	ISO 27701:2019 - Clause 5.3 Leadership Clause 4 Structure of this standard A.5.1 Policies for information security A.5.2 Information security roles and responsibilities A.5.3 Segregation of duties A.5.4 Management responsibilities A.5.24 Information security incident management planning and preparation A.5.25 Assessment and decision on information security events A.5.26 Response to information security incidents A.5.27 Learning from information security incidents A.5.35 Independent review of information security A.5.36 Compliance with policies, rules and standards for information security A.5.37 Documented operating procedures A.8.25 Secure development life cycle A.8.27 Secure system architecture and engineering principles A.8.30 Outsourced development A.8.32 Change management
Risk assessment	Identification and Classification of functions, processes and assets	Requirement 2 (2.4): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 9 (9.6): Restrict physical access to cardholder data Requirement 12 (12.4, 12.5, 12.8, 12.9): Maintain a policy that addresses information security for all personnel	ISO 27005:2022 - A.2.2 Assets Clause 6.1.2 Information security risk assessment A.5.2 Information security roles and responsibilities A.5.9 Inventory of information and other associated assets A.5.10 Acceptable use of information and other associated assets A.5.11 Return of assets A.5.12 Classification of information A.5.13 Labelling of information A.8.32 Change Management

	Risk assessment of functions, processes and assets	Requirement 6 (6.1, 6.6): Develop and maintain secure systems and applications Requirement 10 (10.6): Track and monitor all access to network resources and cardholder data Requirement 11 (11.2, 11.3, 11.5): Regularly test security systems and processes Requirement 12 (12.2, 12.10): Maintain a policy that addresses information security for all personnel	ISO 27005:2022 - A.1.1 Criteria related to risk assessment ISO 27005:2022 - A.1.2 Risk acceptance criteria ISO 27005:2022 - A.2.1 Information security risk components ISO 27005:2022 - A.2.3 Risk sources and desired end state ISO 27005:2022 - A.2.4 Event-based approach ISO 27005:2022 - A.2.5 Asset-based approach ISO 27005:2022 - A.2.6 Examples of scenarios applicable in both approaches ISO 27005:2022 - A.2.7 Monitoring risk-related events ISO 27005:2022 - Clause 8.6.3 Acceptance of the residual information security risk Clause 6.1.2 Information security risk assessment A.6.8 Information security event reporting ISO 27701:2022 - A.5.7 Threat Intelligence A.5.25 Assessment and decision on information security events A.5.26 Response to information security incidents A.5.27 Learning from information security incidents A.5.28 Collection of evidence A.5.29 Information security during disruption A.8.8 Management of technical vulnerabilities A.8.16 Monitoring Activities A.8.32 Change Management
--	---	--	--

Protection			A.5.3 Segregation of duties A.5.14 Information transfer A.5.18 Access rights A.5.31 Legal, statutory, regulatory and contractual requirements A.5.32 Intellectual property rights A.5.33 Protection of records A.5.34 Privacy and protection of PII A.5.35 Independent review of information security A.8.2 Privileged access rights A.8.3 Information access restriction A.8.7 Protection against malware A.8.10 Information deletion A.8.11 Data masking A.8.12 Data leakage prevention A.8.19 Installation of software on operational systems A.8.20 Networks security A.8.21 Security of network services A.8.22 Segregation of network A.8.27 Secure system architecture and engineering principles A.8.29 Security testing in development and acceptance A.8.32 Change Management A.8.34 Protection of information systems during audit testing ISO 27701:2019 - Clause 6.15.1.4 Privacy and protection of personally identifiable information ISO 27701:2019 - Clause 7.2 Conditions for collection and processing ISO 27701:2019 - Clause 7.3 Obligations to PII principals ISO 27701:2019 - Clause 7.4 Privacy by design and privacy by default ISO 27701:2019 - Clause 7.5 PII sharing, transfer and disclosure ISO 27701:2019 - Clause 8.2 Conditions for collection and processing
	Data and Systems Integrity and Confidentiality	Requirement 2 (2.3): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (all): Protect stored cardholder data Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 12 (12.8, 12.9): Maintain a policy that addresses information security for all personnel	
	Access Control	Requirement 6 (6.2): Develop and maintain secure systems and applications Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 8 (all): Identify and authenticate access to system components Requirement 10 (10.2): Track and monitor all access to network resources and cardholder data Requirement 11 (11.5): Regularly test security systems and processes	A.5.3 Segregation of duties A.5.15 Access Control A.5.18 Access rights A.5.17 Authentication information A.8.2 Privileged access rights A.8.3 Information access restriction A.8.5 Secure authentication A.8.15 Logging A.8.16 Monitoring activities A.8.32 Change Management
	Physical Security	Requirement 9 (all): Restrict physical access to cardholder data	A.7 Physical controls

Detection	Incident Monitoring & Reporting	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 12 (12.10): Maintain a policy that addresses information security for all personnel	ISO 27701:2022 - A.5.7 Threat Intelligence ISO 27701:2022 - A.5.24 Information security incident management planning and preparation ISO 27701:2022 - A.5.25 Assessment and decision on information security events ISO 27701:2022 - A.5.26 Response to information security incidents ISO 27701:2022 - A.5.27 Learning from information security incidents ISO 27701:2022 - A.5.28 Collection of evidence ISO 27701:2022 - A.8.15 Logging ISO 27701:2022 - A.8.16 Monitoring activities ISO 27701:2022 - A.8.17 Clock synchronization
	Fraud Detection	Requirement 5 (all): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.1, 6.2, 6.5,6.6): Develop and maintain secure systems and applications Requirement 9 (9.9): Restrict physical access to cardholder data Requirement 10 (all): Track and monitor all access to network resources and cardholder data Requirement 11 (11.1, 11.4, 11.5): Regularly test security systems and processes	ISO 27701:2022 - Clause 9.1 Monitoring, measurement, analysis and evaluation ISO 27701:2022 - A.5.7 Threat Intelligence ISO 27701:2022 - A.7.4 Physical security monitoring ISO 27701:2022 - A.7.5 Protecting against physical and environmental threats ISO 27701:2022 - A.8.15 Logging ISO 27701:2022 - A.8.16 Monitoring activities ISO 27701:2022 - A.8.7 Protection against malware A.8.8 Management of technical vulnerabilities A.8.12 Data leakage prevention A.8.30 Outsourced development
Business continuity	Business Continuity	Requirement 12 (12.10): Maintain a policy that addresses information security for all personnel	A.5.30 ICT readiness for business continuity
Testing of security measures	Testing of Security Measures	Requirement 5 (all): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.1, 6.2): Develop and maintain secure systems and applications Requirement 10 (10.6): Track and monitor all access to network resources and cardholder data Requirement 11 (all): Regularly test security systems and processes Requirement 12 (12.1, 12.11): Maintain a policy that addresses information security for all personnel	Clause 9 Performance evaluation A.5.36 Compliance with policies, rules and standards for information security A.8.8 Management of technical vulnerabilities A.8.29 Security testing in development and acceptance A.8.33 Test information A.8.34 Protection of information systems during audit testing
Security Awareness	Situational Awareness and Continuous Learning	Requirement 6 (6.5): Develop and maintain secure systems and applications Requirement 10 (10.8): Track and monitor all access to network resources and cardholder data Requirement 11 (all): Regularly test security systems and processes Requirement 12 (12.4, 12.5, 12.6, 12.9, 12.10): Maintain a policy that addresses information security for all personnel	ISO 27701:2022 - Clause 7.3 Awareness ISO 27701:2022 - A.5.2 Information security roles and responsibilities ISO 27701:2022 - A.5.7 Threat Intelligence ISO 27701:2022 - A.5.25 Assessment and decision on information security events A.5.27 Learning from information security incidents A.6.3 Information security awareness, education and training A.8.16 Monitoring Activities

Payment service user relationship management	Requirement 12 (all): Maintain a policy that addresses information security for all personnel	Clause 7.3 Awareness A.5.5 Contact with authorities A.5.6 Contact with special interest groups A.5.7 Threat Intelligence A.5.27 Learning from information security incidents A.6.2 Terms and conditions of employment A.6.3 Information security awareness, education and training A.6.5 Responsibilities after termination or change of employment A.8.8 Management of technical vulnerabilities A.8.16 Monitoring Activities A.8.32 Change management
--	---	---

The SCA and CSC are used to compare the two Standards under the scope of PSD2 security measures. PSD2 and SCA, in particular, are fully compliant with PCI DSS Requirements 8.2 and 8.3, which require multi-factor authentication “for non-console access to computers and systems handling cardholder data”. Because of the general shift toward online services, there is a greater need to authenticate users' identities during transactions and banking activities in order to reduce the cost of processing fraudulent transactions, reduce the potential for online fraud, increase cardholder confidence in using online services, and comply with international regulations such as PCI DSS. Concerning PCI DSS compliance, the ECB intends “*to provide interoperable solutions in the European cards market*” through “*specifications developed through industry-driven standardization initiatives*”. PSD2 with SCA, on the other hand, is an important step toward compliance and interoperability for safer online transactions [81]. Furthermore, SCA compliance can be fully covered by ISO/IEC 27001 controls, which prohibit unauthorized access to systems, applications, and the most sensitive network services (e.g., credit card online payment). At the moment, two-factor authentication is the next logical step in maintaining security levels, and by associating this practice with ISO/IEC 27001 controls and recommendations, a stakeholder can keep its information and systems safe from unauthorized entities while remaining in compliance with both the Standard and PSD2 requirements [44]. The use of security credentials for the strong authentication procedure is also safeguarded by the implementation of both PCI DSS and ISO/IEC 27001. Furthermore, because PSC have been designated as “sensitive payment data” by PSD2, it is worthwhile to make a specific reference of the ISO/IEC 27701:2019 Standard, which provides instructions related to privacy information management aspects, including the security and privacy of PSC usage and processing as well as their owners.

According to CSC requirements, such as Open Banking APIs, XS2A procedure, TPPs identification, secure communication channels, and data information exchanged for the purpose of providing payment services, those can be reinforced to a reasonable degree using PCI DSS and ISO/IEC 27001. Furthermore, another ISO 20000 series standard, ISO 20022, can be used in banks' efforts to open up their payment and core banking systems to TPPs. This is also clearly encouraged by the EBA, and it can be utilized specifically by banks when implementing the dedicated XS2A APIs.

PSD2 security measure “Governance” is mapped to many ISO/IEC 27001 controls and introductory clauses of information security organization and policies, as well as each PCI DSS requirement, which is related to configuration Standards, security policies, and operational procedures that should be established. Furthermore, in terms of Governance,

the recently updated ISO 31000 can be used to construct an “effective operational and security risk management framework”, as it provides principles, a structure, and a risk management process. While numerous risk techniques are accessible, the common clause structure of Annex SL has integrated ISO 31000 via all modern management system standards, as well as Leadership as a core principle. However, both can be applied to support PSD2 compliance as well.

According to Risk Assessment, ISO/IEC 27001 outperforms PCI DSS in terms of facilitating PSD2 compliance. Because ISO 27001 is a risk-based standard method for information security management systems, it takes a holistic view of business, process, people, and technology issues throughout the risk mitigation process. Apart from the related ISO 27001 controls, because many areas of PSD2 require an organization to have a good understanding of its business processes, ISO 9001 Quality Management Standard can also provide a strong foundation for PSD2 as well as ISO 27001, which can be built around the same framework. The EBA GLs for Risk Assessment specifically request an inventory of business operations from PSPs. To that aim, the aforementioned can guide and cover the documentation of business activities and assigned roles and responsibilities. PCI DSS regulations, on the other hand, may only cover the monitoring, detection, and review of threats and vulnerabilities that may damage their critical operations and information assets. In order to provide greater PSD2 compliance, the identification of business functions, important roles, supporting processes, and information assets, as well as their classification in terms of criticality, cannot be covered by PCI DSS.

Many ISO/IEC 27001 control areas can be used to ensure the logical security of data and systems, as well as human access, as described by the EBA GLs. Because PSD2 refers to “sensitive payment data” in terms of data, the ISO/IEC 27701:2019 Standard can also play a vital role in this security area, providing stakeholders with reliable guidance on their security and privacy protection. As a result, when compared to PCI DSS, the ISO 27000 series is clearly preferred in its use. Furthermore, the latter is based on the security of information data relating to payment cards (cardholder data) and/or sensitive authentication data. Hence, the appropriate PCI DSS requirements can assist stakeholders have a better understanding of how to develop and adapt the necessary controls surrounding the payment area, including entities, systems, processes, and physical devices, which is the PSD2's goal. Furthermore, PCI DSS has set a very robust data security baseline for all entities involved in payment card processing or the storage, processing, or transmission of the relevant data.

Furthermore, both Standards' controls can provide detection related to incident monitoring and reporting as well as fraud detection. The ISO/IEC 27001 features a separate control section pertaining to incident management, which includes all of the necessary criteria, thresholds, and methodology that must be followed in order to monitor and report the incidents identified. Fraud detection can be accomplished by applying ISO/IEC 27001 and establishing other associated controls in scope. The PCI DSS requirements place a strong emphasis on the entities' ability to use fraud prevention and detection systems. The major Payment Card Schemes (i.e., American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.) include, among others, mechanisms, such as strong authentication, statistical analysis, as well as artificial intelligence applications.

Also, there is a specific control of ISO/IEC 27001:2022 that focuses solely on BCM and provides clear direction on it in the context of PSD2 compliance, whereas PCI DSS support is quite less because only one sub-requirement may be applied. Aside from ISO/IEC 27001

compliance, BCM can be integrated into an ISO 22301 Business Continuity Management System. While ISO 22301 is a relatively recent standard, several financial institutions have implemented a Business Continuity Management System to complement their existing governance structure and provide stakeholder assurance. However, as a key point from the EBA advice also emphasized, for the annual testing of critical functions, processes, systems, transactions, and interdependencies, ISO 22301 is considered more unclear [34].

In terms of the testing framework for the security measures that PSPs should create and apply in accordance with the PSD2, PCI DSS appears to provide more assistance in complying with it. As far as the PCI DSS requirements rely on a payment card-processing ecosystem, and the testing framework encompasses security measures relevant to payment terminals, devices, and software used for payment service provision, for authenticating the PSU, and generating/receiving authentication codes, it covers a broader range of PSD2 requirements. Furthermore, the mapping between PSD2 and PCI DSS could be maximized by implementing the “Regularly test security systems and processes” requirement.

Last but not least, the two investigated Standards can partially encompass security awareness, including PSP situational awareness and continuous learning, as well as PSU awareness of security threats and risk-mitigating actions. Although ISO/IEC 27001 and PCI DSS provide clear guidance in the first case, in the second case, which is associated with PSU relationship management, both include controls assigned to stakeholders' personnel/staff rather than users or customers to whom they provide their services. As a result, while the content of their controls may be used as relevant, the target entity is distinct.

Overall, PCI DSS is a standard for credit cardholder information security, whereas ISO/IEC 27001 is a specification for an information security management system. PSD2 mapping with PCI DSS and ISO/IEC 27001 Standards is critical information for stakeholders responsible with implementing the Directive in their organizations [42]. While this section examined how the two Standards can support PSD2 security measures, meeting any of them alone does not ensure compliance. PCI DSS and ISO/IEC 27001 provide a minimum set of requirements that can be applied in a variety of ways. PSD2's unique requirements for a payment or financial organization must be mapped into the organization's management system framework to ensure that it effectively meets the organization's objectives [34]. In any case, combining PCI DSS and ISO/IEC 27001 is highly recommended as better solutions about information security can be provided to organizations.

Discussion and Conclusions

The introduction of PSD2 into the payment sector provided numerous benefits in terms of information security and data protection. However, practically all MS have found a lack of both harmony and clarity. This explains why banks find it difficult to understand the full spectrum of compliance duties. Although the completion of the EBA RTS was an important milestone that provided firms with greater clarity and certainty on how to move forward with their PSD2 compliance and strategic programs, it still leaves a number of important questions open for stakeholders regarding the technical security specifications on which they should rely and implement in the context of PSD2 compliance.

ASPSPs must make the technical specifications of their access interfaces (whether dedicated or user-facing) available to TPPs, as well as providing them with a testing facility to conduct trials of the software and applications that TPPs will employ to provide services

to their users. Nonetheless, the RTS merely mandates that ASPSPs must guarantee that their interfaces adhere to communication standards set by international or European standardization organizations. However, someone could argue that implementing a common API standard is not always the best solution. To begin, there is a lot of innovation that is helping to overcome open banking fragmentation. One example, albeit maybe unintended in PSD2, is API aggregation. Fintech companies specialize in connecting to bank APIs, creating a single API for other organizations to connect to. This enables other licensed open banking startups to focus on creative user propositions rather than maintaining bank connectivity. The market for both API aggregation and consumer services is very competitive and functional. Second, there is plenty of valuable effort and knowledge within the existing standard bodies, so there is no need to create a new API standard from start. Hence, building on and harmonizing the work of current standards bodies could be a substantial answer, which means that the EU should encourage increased conversation and cooperation between existing standards bodies and PSD2. This way, rather than losing technical and commercial know-how, these groups' technical and commercial know-how would be harnessed, and new standards would align and converge over time, rather than becoming more fragmented. Following the work of the SPAA (SEPA Payment Account Access) MSG (Multi-Stakeholder Group), the EU should additionally define how existing standards organizations should engage with specifications established by the European Payments Council. The connection between PSD2, ISO/IEC 27001:2022, and PCI DSS, which was discussed in the preceding section, is an excellent example of this requirement. It is critical to continue with more such standard mapping actions in order to identify which PSD2 requirement weaknesses (i.e., API standard establishment) should be worked on and improved, as well as which PSD2 security areas are well developed and reinforced based on standard security controls (i.e., ISO/IEC 27001, PCI DSS).

In addition, considering a centralized authority to coordinate API implementation and performance could be a viable alternative. Instead of focusing on a single API standard, the EU may establish a central independent organization or empower existing entities to focus on API implementation and performance across banks. This would be analogous to the Open Banking Implementation Entity in the United Kingdom, which has enforcement powers from the Competition and Markets Authority and aided in the advancement of open banking at a faster rate than other comparable markets. A central independent entity might serve as a single reliable source of open banking data. It is currently difficult to determine how many European users exist, how many payments or data requests are made each month, and how this is changing over time. The OBIE provides this information in the United Kingdom. By giving best practices recommendations, such a group might also help to create more frictionless and uniform payment authentication journeys. Unnecessary difficulty in the verification process is a substantial and artificial barrier to open banking gaining traction in EU [60].

The Commission acknowledges that the lack of more explicit standards is a challenge but considers that it is the obligation of market participants to collaborate to establish a solution that works for all parties [45]. To facilitate this, the Commission has proposed the formation of an Application Programming Interface Evaluation Group (API EG) to evaluate standardized API specifications in order to ensure compliance with PSD2 and other relevant legislation, including the new GDPR, and that they meet the needs of ASPSPs, TPPs, and PSUs. The EU Commission, EBA, and ECB will be observers in the API EG, but will support market participants as needed. The API EG's suggestions and advice will

aim to create standardized market practices throughout EU MSs. Not only would this minimize implementation times and costs for both ASPSPs and TPPs, but it will also be critical for enabling effective cross-border competition based on PSD2-enabled products and services.

Another one issue raised from the PSD2 compliance is that even when the EBA's RTS is released, it is unknown what the authentication technologies will finally look like. The interface to strong authentication outlined in Article 97 PSD2 is expected to be separated from the other technological interfaces outlined in Articles 66 and 67 through the use of a federation protocol such as SAML or OAuth 2.0 and its extension OIDC. While the two protocols differ in technical aspects and represent different standards approaches, both might meet this requirement and serve as the foundation for PSD2-specific interfaces. As a result, it is theoretically possible to establish a comparable PSD2 interface based on both SAML and OAuth 2.0/ OpenID Connect, with technical interfaces based on both SOAP and REST-based web services. Further PSD2 implementation architecture research should focus on secure channel bindings with Holder-of-Key or the newly coming TokenBinding. The trust connection between ASPSPs and TPPs, which is envisioned to use qualified certificates for website authentication or electronic seals, is another critical component of a distributed PSD2 system. While this work only touches on the subject briefly, a more comprehensive treatment that includes information interchange and dynamic discovery using electronic seals and a shared European repository or set of trusted lists has yet to be developed [90].

Furthermore, it is true that PSPs have the authority to rely on the bank's authentication process. The freedom of PSPs to arrange authentication as they see suitable, however, trumps the interest in making this procedure as secure as feasible. While redirection or a decoupled solution may be more secure, the PSD2 and RTS indicate that authentication, including the PSC supplied by the bank, can also be addressed through the PSP using an embedded approach. This interest ordering holds true even if the PSPs employ their own authentication procedure. Although the PSD2 does not clearly indicate this, the bank appears to be compelled to rely on the PSP. The PSD2 and RTS do not need the bank to be able to validate the authentication. It cannot, for example, require a digital signature from the user. The bank only offers a few alternatives for restricting account access. As a result, it has relatively limited authority to prohibit the availability of payment services. However, it also increases the risks. In theory, a criminal can acquire access to an account via any PISP or AISP.

The compromise on the legality of screen scraping leads to the same conclusion. Screen scraping grants a PSP unfettered access to the user's account, even if this access is not required for the payment service to be provided. As a result, the EBA has called for ban. However, the EC has determined that the risk of competition limitation is more significant. If the dedicated interface is not working properly, the adopted RTS allows PSPs to use the user interface. Several restrictions limit this access to the user interface. These controls, however, only allow for ex-post evaluation after the PSP has already had full access. Again, the protection of innovation and competition in the payment services sector takes precedence over the security of payment accounts and user privacy. The probability of an exception has no bearing on the result. After all, a bank may only receive such an exemption if the dedicated interface meets all of the RTS requirements, has been tested by PSPs, has been widely used for at least three months, and any difficulties have been remedied

promptly. If these conditions are met, there is no genuine risk of limiting innovation and competition [86].

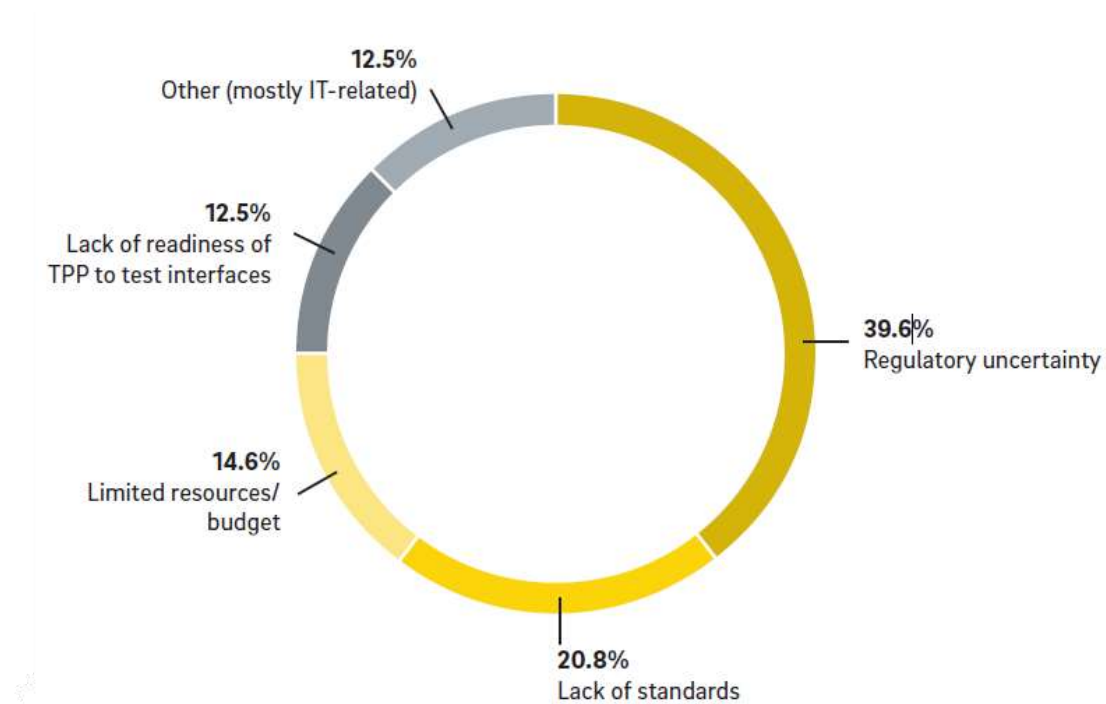


Figure 21. The major challenges or obstacles from the PSD2 implementation [9]

PSD2 was implemented to promote the payments industry by encouraging innovation and extending the market for PSPs. Because TPP services rely on the use of sensitive personal and financial data, it opens up the market to a bigger number of rivals while also relying significantly on the IT infrastructure of various parties, a number of dangers have been identified [85]. Also, previous to PSD2, banks had a monopoly on the financial industry and controlled access to consumer accounts, whilst other PSPs had no legal right to this information. As a result, PSD2 eliminates this competitive advantage, potentially causing problems for banks in the fight against new competition, reduced customer interaction, potential loss of market share, and reduced revenue, as well as problems ensuring customer safety and security in the fight against cyber criminals [73].

While these risks have been recognized, a number of mitigating measures have also been implemented to decrease overall operational risks related to privacy, security, and transaction and fraud risk to an acceptable level. All parties involved in payment services, however, must exercise caution. Furthermore, regulators will play an active role in ensuring a safe and secure payment landscape as part of mitigating market risks through the requirement of particular measures for regulated firms. We should expect the landscape of services, and hence the related risks, to evolve at a quick rate due to the dynamic character of this industry and the rapid development of technology [85]. Nonetheless, banks can capitalize on the fact that they are perceived as sound financial institutions, and if the opportunities allow, they can implement a risk management strategy that will win new markets as technological innovators, or they can choose another strategy, such as collaborating with FinTech companies, which potentially can bring certain benefits in the provision of a range of innovative payment products and services [73].

However, determining which potential risks and concerns come from PSD2 implementation is crucial. In general, PSD2 is harmful to banks since, as ASPSPs, they are expected to build, manage, and provide a system that permits access to customer information, as well as refund an unlawful or erroneous payment transaction, even if the transaction was begun through a PISP. Banks invest much on security because their brand is at stake. However, while banks have strong security, third-party applications are not subjected to the same scrutiny and do not prioritize security; however, because banking applications must provide APIs for third-party applications, they need adhere to the same security standard. This is also illustrated by the fact that card schemes and e-merchants are putting pressure on the SCA rules to be postponed yet more. In any case, even granting TPPs access to banks' APIs does not guarantee 100% payment service security and exposes potential cyber adversaries to a far greater attack surface. Critical programs can no longer be hidden behind perimeter firewalls. Every application accessible for download is especially vulnerable because hackers can isolate it in a sandbox environment and repeatedly assault it until they crack its protection. Once an application has been compromised and APIs have been used to access it, cybercriminals can use it to deceive the system into thinking they are a valid client and gain access to anything that the API is authorized to connect to. Code fixing procedures must be implemented to prevent cheating [77][73]. In addition, Andrew Whaley, Vice President of Arxan and former lead engineer at Barclays Bank, expresses concern about AISP that will not only acquire access to bank users' data, but will also be able to collect and store it on their servers, from where it might be stolen [31].

Banks, on the other hand, face new competition, with PSD2 reducing their capacity to sell other products or services due to the loss of market share in favor of AISP and PISP, as well as their revenue due to competitive pricing, detect fraud, and reduce their institutional role in their customers' everyday lives.

Moreover, while adhering to PSD2 rules, the banking industry will need to discover a mechanism to assure secure data access and permission management while preventing application manipulation. PSD2 makes it quite apparent that banks would be held accountable for the ownership, security, and confidentiality of client data. To access payment accounts (e.g., current accounts) and statement details, as well as other account information maintained by banks and other ASPSPs where consumers consent to such access, traditional PSPs must share some data with those TPPs. Although some of that data is considered personal data under the GDPR, the sharing requirements result in some tension between the two sets of standards. Even when both legislative frameworks get into force, significant questions remain [75]. As a result, consumers' personal information is ultimately not effectively protected. On the one hand, account access is restricted in a variety of ways, and the GDPR extends to the provision of payment services. The term of "account information service" is, however, broad and encompasses a wide range of services. This promotes innovation in the payment services business while also allowing PSPs to avoid account access constraints. Furthermore, the PSD2 does not address the privacy implications of large-scale account information processing [86]. Another issue that arises in relation to the exploitation of the user's consent is that corporations may utilize payment information without the user's consent or seek to get their implicit consent in a discrete manner. For example, they may utilize the data for purposes not explicitly stated or presented to the user in a hazy manner, etc. Concerns have also been raised in

circumstances where consumers revoke previously granted consent to Fintech or request the removal of their personal payment data from the database.

Overall, PSD2 has established and effectively regulated new financial market participants and encouraged the creation of new financial services. It has broadened the scope of payments from exclusively EU/EEA domestic currency payments to payments in all currencies if at least one participant is located on EU/EEA territory. Furthermore, it has introduced new licensing standards for TPPs and prohibited financial service providers from accessing users' accounts without their express authorization. The implementation of RTS has increased the security of payment processing via SCA regulations. Opening the banking industry to required APIs, which require banks to offer third parties who want to enter the market with information about their clients, would accelerate market digitization and innovation, but it will also place banks in a difficult position from the scope of security and protection. In an era where technology is constantly evolving, the majority of banking transactions are performed through digital payment transfer platforms (i.e., APIs), and thus banks become the primary target of cyberattacks, it is critical for the PSD2 to take preventive security measures against potential threats that will be even more IT related and associated with other security standards. In this way, banks will be able to better respond to the technological needs of the development and implementation of Open Banking APIs, and they will be able to be more certain about which measures should be taken holistically and aggregately in order to be PSD2 compliant [73].

References

- [1] “Directive (EU) 2015/2366 of the European Parliament and of t... - EUR-Lex.” <https://eur-lex.europa.eu/EN/legal-content/summary/revised-rules-for-payment-services-in-the-eu.html> (accessed Jan. 10, 2023).
- [2] “Directive 2015/2366 - Payment services in the internal market - EU monitor.” https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk0vn25mntsj (accessed Jan. 10, 2023).
- [3] “The Ultimate Guide to Online Payment Processing.” <https://www.2checkout.com/lp/online-payment-processing-guide/> (accessed Jan. 11, 2023).
- [4] “Frequently Asked Questions: PSD2,” *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555 (accessed Jan. 11, 2023).
- [5] “What Is the PSD2 Regulation? Purpose & Compliance | Sectigo® Official.” <https://sectigo.com/resource-library/the-revised-payment-services-directive-psd2-explained> (accessed Jan. 11, 2023).
- [6] “Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electro,” *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/pl/MEMO_17_4961 (accessed Jan. 11, 2023).
- [7] “PSD2 Requirements through the Technical Security Lens.” <https://cyscale.com/blog/PSD2-technical-requirements/> (accessed Jan. 11, 2023).

- [8] “Payment Services Directive 2 - all you need to know.” <https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know> (accessed Jan. 11, 2023).
- [9] Ronald Berger, “Adapt or die? Why PSD2 has so far failed to unlock the potential of Open Banking,” 2019. https://www.rolandberger.com/publications/publication_pdf/roland_berger_psd2.pdf (accessed Jun. 02, 2023).
- [10] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)*. 2015. Accessed: Jan. 11, 2023. [Online]. Available: <http://data.europa.eu/eli/dir/2015/2366/2015-12-23/eng>
- [11] “Payment Services Directive: frequently asked questions,” *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/de/MEMO_15_5793 (accessed Jan. 11, 2023).
- [12] “Three ways PSD2 will benefit consumers,” *UK Finance*. <https://www.ukfinance.org.uk/blogs/three-ways-psd2-will-benefit-consumers> (accessed Jan. 11, 2023).
- [13] kjadmin, “PSD2 license explained: services, types of licenses, application,” *Advapay*, Aug. 19, 2021. <https://advapay.eu/psd2-license-payment-service-directive-explained-service-types-of-license-application/> (accessed Jan. 11, 2023).
- [14] “Non-bank PSP license (EMI Licence/PI License) - PSP Lab,” Mar. 04, 2020. <https://psplab.com/services/pi-emi-authorisation/> (accessed Jun. 06, 2023).
- [15] BBVA, “Everything you need to know about PSD2 | BBVA,” *NEWS BBVA*, Oct. 16, 2019. <https://www.bbva.com/en/everything-need-know-psd2/> (accessed Jan. 11, 2023).
- [16] “Open Banking: AISP, PISP & ASPSP Explained - Macro Global,” May 18, 2022. <https://www.macroglobal.co.uk/blog/regulatory-technology/open-banking-psd2/aisp-pisp-aspsp-explained/> (accessed Jan. 11, 2023).
- [17] “PSD2.” <https://www.reply.com/technology-reply/en/content/psd2> (accessed Jan. 11, 2023).
- [18] “What is an electronic money institution (EMI)? Beyond traditional banking,” *Verified Payments*, May 12, 2021. <https://verifiedpayments.com/blog/beyond-traditional-banking-what-is-an-electronic-money-institution-emi/> (accessed Jan. 11, 2023).
- [19] “Open Banking Europe: Registration & Passporting Open Banking Europe - providing collaborative services to support PSD2 Access to Account (XS2A), in partnership with the financial industry”, Open Banking Europe, Jan. 18, 2021. <https://www.openbankingeurope.eu/media/1935/obe-psd2-xs2a-registration-passporting-guide.pdf> (accessed Jan. 11, 2023).
- [20] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and*

repealing Directive 2007/64/EC (Text with EEA relevance). 2015. Accessed: Jan. 11, 2023. [Online]. Available: <http://data.europa.eu/eli/dir/2015/2366/2015-12-23/eng>

[21] “What is PSD2 Compliance and What Does it Mean for Your Business?” <https://www.varonis.com/blog/psd2> (accessed Jan. 11, 2023).

[22] “EBF PSD2 Guidance Final December 2019 | PDF | Payments | European Union,” Scribd. <https://www.scribd.com/document/534126697/EBF-PSD2-guidance-Final-December-2019> (accessed Jan. 11, 2023).

[23] “PSD2 – Payment Services Directive 2 What is new?,” *Deloitte*, 2016. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu_psd2-payment-services-directive2.pdf (accessed Jan. 11, 2023).

[24] “Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance),” <https://webarchive.nationalarchives.gov.uk/eu-exit/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015L2366-20151223>. <https://www.legislation.gov.uk/eudr/2015/2366/contents> (accessed Jan. 11, 2023).

[25] “Payment instrument (Definitions, PSD2) | Lewik.” <https://www.lewik.org/term/16192/payment-instrument-definitions-psd2/> (accessed Jan. 11, 2023).

[26] “EBF PSD2 Guidance September 2016 | PDF | Payments | European Union,” Scribd. https://www.ebf.eu/wp-content/uploads/2017/05/EBF_PSD2_guidance_September_2016.pdf (accessed Jan. 11, 2023).

[27] “Guidelines on authorisation and registration under PSD2,” *European Banking Authority*, Jul. 11, 2017. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2> (accessed Feb. 01, 2023).

[28] “Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee,” *European Banking Authority*, Jul. 07, 2017. <https://www.eba.europa.eu/guidelines-on-the-criteria-on-how-to-stipulate-the-minimum-monetary-amount-of-the-professional-indemnity-insurance-under-ps-2> (accessed Feb. 01, 2023).

[29] “PSD2 authorisation and registration – clarity at the EU and UK level?” <https://www.osborneclarke.com/insights/psd2-authorisation-and-registration-clarity-at-the-eu-and-uk-level> (accessed Feb. 01, 2023).

[30] “Authorisation and registration: e-money institutions (EMI) and PIs (PI),” *FCA*, Oct. 15, 2015. <https://www.fca.org.uk/firms/authorisation-registration-emoji-payment-institutions> (accessed Feb. 01, 2023).

[31] S. Mansfield-Devine, “Ransomware: taking businesses hostage,” *Network Security*, vol. 2016, no. 10, pp. 8–17, Oct. 2016, doi: [10.1016/S1353-4858\(16\)30096-4](https://doi.org/10.1016/S1353-4858(16)30096-4).

- [32] “Recital,” *European Banking Authority*, Jul. 09, 2019. <https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/5404> (accessed Feb. 01, 2023).
- [33] “Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance),” <https://webarchive.nationalarchives.gov.uk/eu-exit/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015L2366-20151223>. <https://www.legislation.gov.uk/eudr/2015/2366/annex/I> (accessed Jun. 06, 2023).
- [34] R. Clements, “Supporting PSD2 Compliance with ISO Certification,” *Assent Risk Management*, Nov. 21, 2018. <https://www.assentriskmanagement.co.uk/supporting-psd2-compliance-with-iso-certification/> (accessed Jun. 06, 2023).
- [35] Information technology — Security techniques — Information security management systems — Requirements, INTERNATIONAL STANDARD ISO/IEC 27001, Reference number ISO/IEC FDIS 27001:2013(E). <http://www.itref.ir/uploads/editor/42890b.pdf> (accessed Jun. 06, 2023).
- [36] “Regulatory Technical Standards on Home-Host cooperation under PSD2,” *European Banking Authority*, Jul. 31, 2018. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/rts-on-home-host-cooperation-under-psd2> (accessed Feb. 01, 2023).
- [37] “Regulatory Technical Standards on passporting under PSD2,” *European Banking Authority*, Dec. 14, 2016. <https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-of-branches/regulatory-technical-standards-on-passporting-under-psd2> (accessed Feb. 01, 2023).
- [38] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)*, vol. 337. 2015. Accessed: Feb. 01, 2023. [Online]. Available: <http://data.europa.eu/eli/dir/2015/2366/oj/eng>
- [39] Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1, *PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL*, June 2019. <https://listings.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf> (accessed Jun. 06, 2023).
- [40] “Directive (EU) 2015/849 of the European Parliament and of th... - EUR-Lex.” <https://eur-lex.europa.eu/EN/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes.html> (accessed Feb. 01, 2023).
- [41] “Regulatory Technical Standards on central contact points under PSD2,” *European Banking Authority*, Dec. 11, 2017. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/rts-on-central-contact-points-under-psd2> (accessed Feb. 01, 2023).

- [42] “Comparison of PCI DSS and ISO/IEC 27001 Standards,” vol. 1, 2016. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2016/volume-1/comparison-of-pci-dss-and-iso-iec-27001-standards_joa_eng_0116
- [43] “Technical Standards on the EBA Register under PSD2,” *European Banking Authority*, Apr. 10, 2019. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/technical-standards-on-the-eba-register-under-psd2> (accessed Feb. 01, 2023).
- [44] R. Leal, “ISO 27001 access control – Using two-factor authentication.” <https://advisera.com/27001academy/blog/2017/01/16/how-two-factor-authentication-enables-compliance-with-iso-27001-access-controls/> (accessed Jun. 06, 2023).
- [45] “PSD2 finalised standard on SCA and CSC: the wait is over, but questions remain | Deloitte Cyprus | Financial Services,” *Deloitte Cyprus*. <https://www2.deloitte.com/cy/en/pages/financial-services/articles/psd2-finalised-standard-on-sca-and-csc.html> (accessed Jun. 06, 2023).
- [46] “FCA finalises revised Payment Services Directive (PSD2) requirements,” *FCA*, Sep. 18, 2017. <https://www.fca.org.uk/news/press-releases/fca-finalises-revised-psd2-requirements> (accessed Feb. 01, 2023).
- [47] “PSD2 & Open Banking Security and Fraud Impacts on Banks”.
- [48] “Payment services and electronic money,” *European Banking Authority*. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money> (accessed Feb. 01, 2023).
- [49] “Regulatory Technical Standards on passporting under PSD2,” *European Banking Authority*, Nov. 20, 2017. <https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-of-branches/regulatory-technical-standards-on-passporting-under-psd2> (accessed Feb. 01, 2023).
- [50] “Regulatory Technical Standards on central contact points under PSD2,” *European Banking Authority*, Aug. 14, 2018. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/rts-on-central-contact-points-under-psd2> (accessed Feb. 01, 2023).
- [51] “Guidelines on procedures for complaints of alleged infringements of the PSD2,” *European Banking Authority*, Dec. 05, 2017. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-procedures-for-complaints-of-alleged-infringements-of-the-psd2> (accessed Feb. 01, 2023).
- [52] “Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2,” *European Banking Authority*, Sep. 12, 2017. <https://www.eba.europa.eu/guidelines-on-the-criteria-on-how-to-stipulate-the-minimum-monetary-amount-of-the-professional-indemnity-insurance-under-ps-2> (accessed Feb. 01, 2023).
- [53] “Technical Standards on the EBA Register under PSD2,” *European Banking Authority*, Apr. 10, 2019. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/technical-standards-on-the-eba-register-under-psd2> (accessed Feb. 01, 2023).

- [54] E. C. Bank, “The revised Payment Services Directive (PSD2),” *European Central Bank*, Oct. 05, 2018. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html (accessed Feb. 01, 2023).
- [55] “PSD2 regulation - Get ready with Thales,” *Thales Group*. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2> (accessed Feb. 01, 2023).
- [56] “The SCA card deadline is here: your questions answered | TrueLayer.” <https://truelayer.com/blog/the-sca-deadline-for-cards-is-here-your-sca-questions-answered/> (accessed Feb. 01, 2023).
- [57] “The EBA reminds financial institutions of the need for readiness in view of the Brexit transition period ending on 31 December 2020,” *European Banking Authority*, Nov. 06, 2020. <https://www.eba.europa.eu/eba-reminds-financial-institutions-need-readiness-view-brexit-transition-period-ending-31-december> (accessed Feb. 01, 2023).
- [58] “Directive (EU) 2015/2366 of the European Parliament and of t... - EUR-Lex.” <https://eur-lex.europa.eu/EN/legal-content/summary/revised-rules-for-payment-services-in-the-eu.html> (accessed Feb. 01, 2023).
- [59] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)*. 2015. Accessed: Feb. 01, 2023. [Online]. Available: <http://data.europa.eu/eli/dir/2015/2366/2015-12-23/eng>
- [60] “TrueLayer Blog: PSD2: does Europe need a single API standard?” <https://truelayer.com/blog/product/psd2-does-europe-need-a-single-api/> (accessed Jun. 06, 2023).
- [61] S. M. Slinn Michaela Nebel, Benjamin, “European Union: How does PSD2 interplay with the GDPR?,” *Global Compliance News*, Oct. 23, 2020. <https://www.globalcompliancenews.com/2020/10/23/european-union-how-does-psd2-interplay-with-the-gdpr/> (accessed Jun. 06, 2023).
- [62] B. Geva, “Payment Transactions under the E.U. Second Payment Services Directive – An Outsider’s View.” Rochester, NY, 2019. Accessed: Jun. 02, 2023. [Online]. Available: <https://papers.ssrn.com/abstract=3292313>
- [63] R. Steennot, “Reduced payer’s liability for unauthorized payment transactions under the second Payment Services Directive (PSD2),” *Computer Law & Security Review*, vol. 34, no. 4, pp. 954–964, Aug. 2018, doi: [10.1016/j.clsr.2018.05.008](https://doi.org/10.1016/j.clsr.2018.05.008).
- [64] B. Geva, “Title IV: Rights and Obligations in Relation to the Provision and Use of Payment Services (Chapter 3, Arts 78-93): execution of payment transactions.” Rochester, NY, 2021. Accessed: Jun. 02, 2023. [Online]. Available: <https://papers.ssrn.com/abstract=4160905>
- [65] “U.C.C. - ARTICLE 4A - FUNDS TRANSFER (2012),” *LII / Legal Information Institute*. <https://www.law.cornell.edu/ucc/4A> (accessed Jun. 02, 2023).
- [66] “Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation”, 2016, *PCI Security Standards Council*.

https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&ved=0CAIQw7AJahcKEwig2tfNla7_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.pcisecuritystandards.org%2Fdocuments%2FGuidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf&psig=AOvVaw1mrHdUypyMhXEocFdax0E1&ust=1686124557998625 (accessed Jun. 02, 2023).

[67] “PCI DSS Compliance and Certification - 7Security.”
https://www.7sec.com/compliance/pci-dss/?gclid=Cj0KCQjwyt-ZBhCNARIsAKH11740YKQHIJhpgaW30yK_gycT5KEFEQIFFe9yJ9iGayrwWZ6krW4r1ZsaAlW9EALw_wcB (accessed Jun. 02, 2023).

[68] “PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.”, 2019, *PCI Security Standards Council, LLC*.
https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&ved=0CAIQw7AJahcKEwi4zfiLla7_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.pcisecuritystandards.org%2Fpdfs%2Fpci_ssc_quick_guide.pdf&psig=AOvVaw3dstyJK4m1ZooeF6keFJPb&ust=1686124357113092 (accessed Jun. 02, 2023).

[69] F. Caron, “Specific theme : endpoint security : a comparative overview of approaches to reduce payment fraud,” 2018. Accessed: Jun. 02, 2023. [Online]. Available: <https://www.semanticscholar.org/paper/Specific-theme-%3A-endpoint-security-%3A-a-comparative-Caron/4ab0d83a55a28f55c0eb6f9ca8750fd5bf329992>

[70] “FINTECH SURVEY OF THE ITALIAN FINANCIAL SYSTEM”, BANCA D’ITALIA, November 2021. https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2021/Rilevazione_fintech_2021_EN.pdf?language_id=1 (accessed Jun. 06, 2023).

[71] “Preparing for PSD2 SCA”, *Visa*, November 2018.
https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwjYzcXOmK7_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.visa.co.uk%2Fdam%2FVCOM%2Fregional%2Fve%2Fuk%2Fpdf%2Fvisa-preparing-for-psd2-sca-publication-version-1-1-05-12-18-002-final.pdf&psig=AOvVaw0rC-fop-05z1gG9QkMpL0x&ust=1686125362274063 (accessed Jun. 06, 2023).

[72] solidpixels <https://www.solidpixels.com>, “PSD2: The Role of Authentication Codes in Strong Customer Authentication,” *Wultra*. <https://www.wultra.com/blog/psd2-the-role-of-authentication-codes-in-strong-customer-authentication> (accessed Jun. 06, 2023).

[73] M. Petrovic, “PSD2 influence on digital banking transformation: Banks’ perspective,” *Journal of Process Management. New Technologies*, vol. 8, pp. 1–14, Oct. 2020, doi: [10.5937/jouproman8-28153](https://doi.org/10.5937/jouproman8-28153).

[74] “Privacy at the epicentre”, *Deloitte*, June 2018.
https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwi47-agmK7_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fau%2FDocuments%2Ffinancial-services%2Fdeloitte-au-fs-open-banking-privacy-epicentre-170718.pdf&psig=AOvVaw2NiSRle8pitmcjqZGcB3os&ust=1686125246286728 (accessed Jun. 06, 2023).

- [75] “Second Payment Services Directive and the General Data Protection Regulation – Payments and Consent for Data Sharing”, *Squire Patton Boggs*, January 2019 <https://www.squirepattonboggs.com/-/media/files/insights/publications/2019/01/second-payment-services-directive-and-the-general-data-protection-regulation-payments-and-consent-for-data-sharing/secondpaymentservicesdirectiveandthegeneraldataprotectionregulation.pdf?rev=880fee6379604a048b1e97b154d9dd42> (accessed Jun. 06, 2023).
- [76] “Guidelines on major incidents reporting under PSD2,” *European Banking Authority*, Dec. 19, 2017. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2> (accessed Jun. 06, 2023).
- [77] “PSD2 & Open Banking Security and Fraud Impacts on Banks”. https://www.accenture.com/_acnmedia/pdf-40/accenture-psd2-open-banking-security-fraud-impacts.pdf (accessed Jun. 02, 2023).
- [78] “EBA publishes Opinion on obstacles to the provision of third party provider services under the Payment Services Directive,” *European Banking Authority*, Jun. 04, 2020. <https://www.eba.europa.eu/eba-publishes-opinion-obstacles-provision-third-party-provider-services-under-payment-services> (accessed Apr. 15, 2023).
- [79] “EBA publishes an Opinion on the elements of strong customer authentication under PSD2,” *European Banking Authority*, Jun. 21, 2019. <https://www.eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2> (accessed Apr. 15, 2023).
- [80] O. Maas, “How to handle EBA Guidelines on internet payment security to prepare PSD2”.
- [81] “Additional Time Period for the Implementation of the Requirements for Strong Customer Authentication Standards of Delegated Regulation (EU) 2018/389 – Kyriakides Georgopoulos Law Firm.” <https://kglawfirm.gr/additional-time-period-for-the-implementation-of-the-requirements-for-strong-customer-authentication-standards-of-delegated-regulation-eu-2018-389/> (accessed Apr. 15, 2023).
- [82] V. Bhatt, “eIDAS Qualified Certificates Under PSD2 Frequently Asked Questions,” *Open Banking Exchange*, Jan. 18, 2021. <https://www.openbanking.exchange/europe/resources/publications/eidas-qualified-certificates-under-psd2-frequently-asked-questions/> (accessed Apr. 15, 2023).
- [83] “Are you PSD2-Ready? A guide to the latest information and sources of support – Corporates and Institutions.” https://corporates.db.com/publications/White-papers-guides/are-you-psd2-ready-a-guide-to-the-latest-information-and-sources-of-support?language_id=1 (accessed Apr. 15, 2023).
- [84] ant, “PSD2 - Security Obligations,” *EmoneyAdvice*, Jul. 08, 2017. <http://emoneyadvice.com/psd2-security/> (accessed Apr. 15, 2023).
- [85] “PSD2 risks and IT controls to mitigate,” *Compact*. <https://www.compact.nl/en/articles/psd2-risks-and-it-controls-to-mitigate/> (accessed Apr. 15, 2023).

- [86] P. T. J. Wolters and B. P. F. Jacobs, “The security of access to accounts under the PSD2,” *Computer Law & Security Review*, vol. 35, no. 1, pp. 29–41, Feb. 2019, doi: [10.1016/j.clsr.2018.10.005](https://doi.org/10.1016/j.clsr.2018.10.005).
- [87] M. Petrović, “PSD2 influence on digital banking transformation: Banks’ perspective,” *J Process Man, New Technol*, vol. 8, no. 4, pp. 1–14, 2020, doi: [10.5937/jouproman8-28153](https://doi.org/10.5937/jouproman8-28153).
- [88] H. Özgür, “PERSONAL DATA PROCESSING BY THIRD PARTY PROVIDERS IN ONLINE PAYMENT TRANSACTIONS UNDER GDPR AND PSD2 AN IN-DEPTH LEGAL ANALYSIS FOR GDPR AND PSD2 COMPLIANCE”.
- [89] “Strong Customer Authentication and common and secure communication under PSD2”.
- [90] D. Hühnlein, “Towards secure and standard-compliant implementations of the PSD2 Directive,” 2017.
- [91] *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance.)*, vol. 069. 2017. Accessed: Apr. 15, 2023. [Online]. Available: http://data.europa.eu/eli/reg_del/2018/389/oj/eng
- [92] “Regulatory Technical Standards on strong customer authentication and secure communication under PSD2,” *European Banking Authority*, Apr. 12, 2019. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2> (accessed Apr. 15, 2023).
- [93] “Guidelines on security measures for operational and security risks under the PSD2,” *European Banking Authority*, Jan. 12, 2018. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2> (accessed Apr. 15, 2023).
- [94] “Guidelines on ICT and security risk management,” *European Banking Authority*, Dec. 13, 2018. <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management> (accessed Apr. 15, 2023).
- [95] V. Bhatt, “TPP User Management for PSD2 Access to Account (XS2A),” *Open Banking Exchange*, Jul. 19, 2022. <https://www.openbanking.exchange/europe/resources/publications/tpp-user-management-for-psd2-xs2a/> (accessed Apr. 15, 2023).