Exploring the Dynamics of Payment Services Directive 2 (PSD2) and examining its core tenets

Abstract:

This report offers an examination of various facets of Payment *Services Directive 2 (PSD2)* and delves into its key aspects. The report also encompasses the emergence and role of the *Third Party Service Provider* in the market as *Account Information Service Provider (AISP)* & *Payment Initiation Service Providers (PISP),* the implementation of *Strong Customer Authentication (SCA)* process. The report outlines the critical challenges of timely and comprehensive reporting to be made to the *Central Bank* under PSD2. As well there is necessity to scan the access of the Account Servicing *Payment Service Providers (ASPSP)* who requires permission through API's to collect information of bank's internal customer base. The report encompasses the advantages of Reg-Tech companies who can ensure entire monitoring and reporting framework without relying solely on manual tracking. The state-of-art *Artificial Intelligence (AI) and Software as a Service (SaaS)* tools as used by the RegTech companies can provide advanced risk assessment capabilities that can help a financial institute to manage risks associated with PSD2 compliance with much ease. Further the RegTech platforms can help to maintain a comprehensive audit trail and documentation of activities related to PSD2 compliance. These not only facilitate internal auditing processes but also provide evidence of compliance to regulatory authorities and avoid any unwarranted situations as well.

Glossary

1. Account Information Service Provider (AISP): An entity authorized under the PSD2 to access and aggregates a user's financial information from multiple sources, with the user's consent.
2. Artificial Intelligence (AI): A branch of computer science that aims to create intelligent machines capable of performing tasks that typically require human intelligence.
3. Cash in Transit (CIT) Co: Specialized firms responsible for secure transportation of cash, valuables and other high-value items between locations such as banks, businesses and ATMs.
4. Cash Management Service (CMS) Co: Specialized firms that provide comprehensive solutions for managing cash and liquidity for businesses, financial institutions, and other organizations.
5. European Central Bank (ECB): The central bank for the eurozone, responsible for monetary policy and overseeing the stability of the euro currency.
6. European Union Commission: The executive body of the European Union (EU) responsible for proposing legislation, implementing decisions, upholding EU treaties.
7. Incident Reporting: Process of documenting and communicating events or occurrences that deviate from normal operations, standards or expectations within an organization.
8. Payment Initiation Service Provider (PISP): An entity authorized under the PSD2 to initiate payment transactions on behalf of a user, with the user's explicit consent.
9. Payment Services Directive (PSD): PSD is an EU regulation that aims to modernize payment services in Europe.
10. Software as a Service (SaaS): A software delivery model where applications are hosted by a third-party provider and made available to customers over the internet on a subscription basis.
11. Strong Customer Authentication (SCA): A security measure mandated by the PSD2 requiring two or more authentication factors to validate the identity of an user during electronic transaction.

CONTENTS

Introduction:

Payment Services Directive 2 (PSD2), a landmark regulatory framework that has significantly reshaped the landscape of financial services within the European Union (EU). The report helps to equip with the necessary insights and make informed decisions to strategically navigate the dynamic landscape shaped by PSD2 in financial payment system across EU. Further exploration of PSD2 and aligning with the directive's principles, ensuring compliance and embracing the opportunities for growth, there is necessity to closely monitor and timely reporting to avoid any compliance failure resulting financial and reputation loss.

Background of PSD2:

P*SD 1* was the first the *Payment Services Directive (EU) 2007/64/EC* passed by the EU Council which came into force in 2009, was primarily to set uniform rules for certain types of electronic payments including credit transfers, direct debits, card payments and mobile and online payments etc.

However the *EU Commission* and *European Central Bank* soon realized there is significant technical innovation with rapid growth in the number of electronic and mobile payments and the emergence of new types of payment services in the market place that is challenging the current framework as set in PSD 1. There was an urgent need to make such internet payment procedures easier and safer for growing number of consumers across EU. The primary focus will be to protect consumers against any fraud or abuse that can impact any point due to such innovations across financial market. And to arrest the situation the EU Commission came up with *Payment Services Directive 2* in the year 2015.

Transposed to Irish Law:

Acting in accordance with Ordinary Legislation Procedure with regard to the proposal of European Commission and simultaneous opinion of the European Central Bank, on 25 November 2015, the European Parliament and European Council has complemented the legal framework for payment services under PSD1 with further amendment to Directive 2015/2366/EU on payment service, often referred as PSD2, to provide a strong legal foundation for the future progress of a better integrated and controlled internal market for electronic payments within the European Union (EU).

The Central Bank of Ireland has transposed PSD2 into Irish law by Statutory Instrument No. 6 of 2018, the European Union (Payment Services) Regulations 2018 (PSR), which became effective in Ireland on 13 January 2018.

The primary aims of the Directives are very transparent and clear:

- Controlled and integrated internal market for electronic payments within EU.
- Setting comprehensive framework for payment service with goal of making payment more efficient and secures within EU.
- Providing greater protection to consumers by enhancing security measures of electronic payment.
- Seek to open up payment market for new entrants as Open Banking platform with view to encourage more competition, greater choice and better price for consumers.

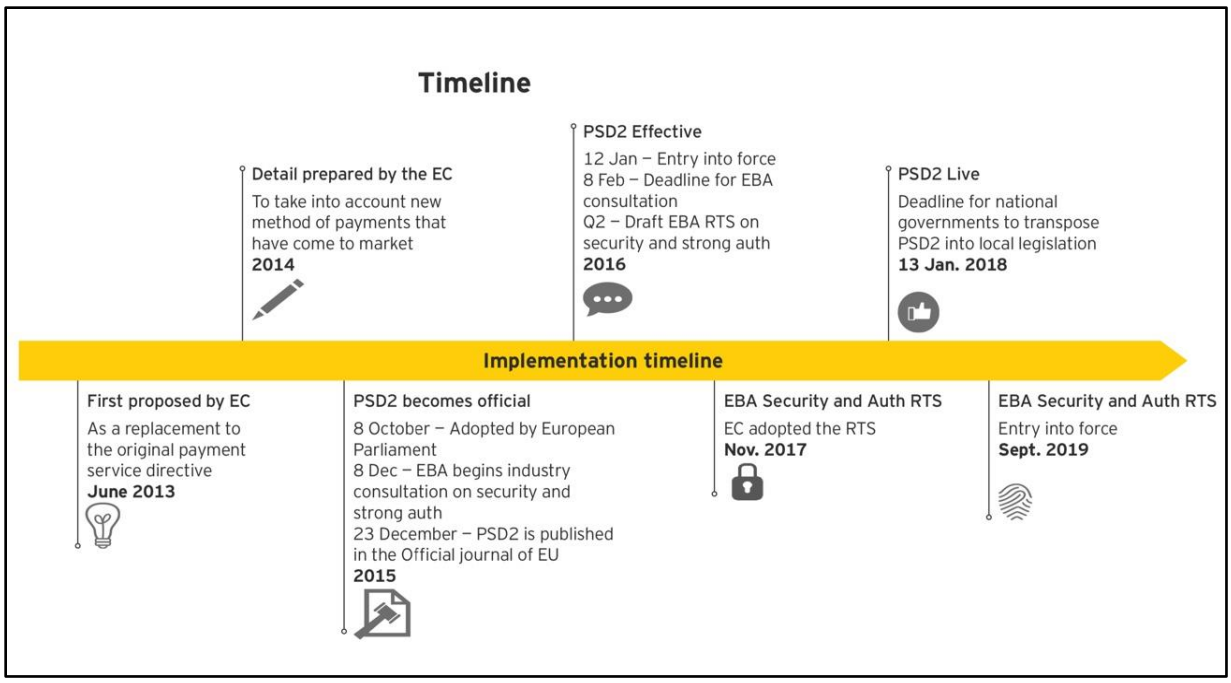

Image source- assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/bcm-pdf/ey-regulatory-agenda-updates.pdf

Objective of PSD2:

With PSD2, the EU Commission has attempted to close the regulatory gaps by generating more legal clarity with a consistent application of the legislative framework across the Union. This has not only guaranteed equivalent operating conditions for existing financial institutes but also opened access to several new players on the market. This new Directive enabled new means of payment to cater broader market while ensuring a high level of consumer protection in the use of those payment services. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonized payments market. This Directive is not applicable to the activities of *Cash-in-Transit companies (CIT)* and *Cash Management Service (CMS)* companies where the activities concerned are limited to the physical transport of banknotes and coins.

Role and Responsibilities under PSD2:

The PSD2 has introduced certain new concepts in the banking eco system that has changed the entire functionality of the traditional banks with advent of Open Banking system and entry of *Third Party Provider's (TPP) - Account Information Service Providers (AISP's)* and *Payment Initiation Service Providers (PISP's)* who are collectively referred as *Account Servicing Payment Service Providers (ASPSP)* in the financial landscape. At the same time PSD2 has also enhanced the customer security system with Strong Customer Authentication (**SCA**) means an authentication based on the use of two or more elements categorized as *Knowledge* (something only the user knows), *Possession* (something only the user possesses) and *Inherence* (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data*. (Directive (EU) 2015/2366 of the European Parliament and of the council, 25 November 2015).*

PSD2 has directed that all *Payment Service Providers (PSP)* must ensure personalized security credentials for its all users for purpose of authenticating any financial transactions initiated by them. It has been categorically highlighted that if the payment service provider of the payee or account holder fails to accept *Strong Customer Authentication*, then they are liable to refund the financial damage caused to the payor or remitter due to any unprecedented fraudulent activity *(PSD2 point (b) of Article 69/1).*

One of the most critical aspects of *PSD2* is considered to be the regulation of *'Access to Account'.* The provision of a regulated access to a payor account for payment initiation services (PIS) as well as account information services (AIS) has created a huge business opportunities for established and new market competition to improve, enlarge or even re-engineer the current product and service architecture available in this domain.

Payment Initiation Service Providers (PISP's) are financial institutions that help consumers to make online credit transfers and inform the merchant instantly of the payment initiation. This process enables immediate dispatch of goods or immediate access to services as purchased online. For online payments, PISP's constitute an alternative to credit card payments that offer an easily accessible payment service, as the consumer only needs to possess an online payment account. *(centralbank.ie/regulation/psd2-overview/faq)*

Responsibilities of Payment Initiation Services Provider (PISP's)

- Initiate payment (credit transfers) by means of the IT infrastructure or API applications of a third party provider.
- Empowered to access the payment accounts of the payee via online.
- Explicit payor consent prior to initiate any payment in form of SCA.
- No dependence on a contractual relationship between PISP and account servicing payment service provider.

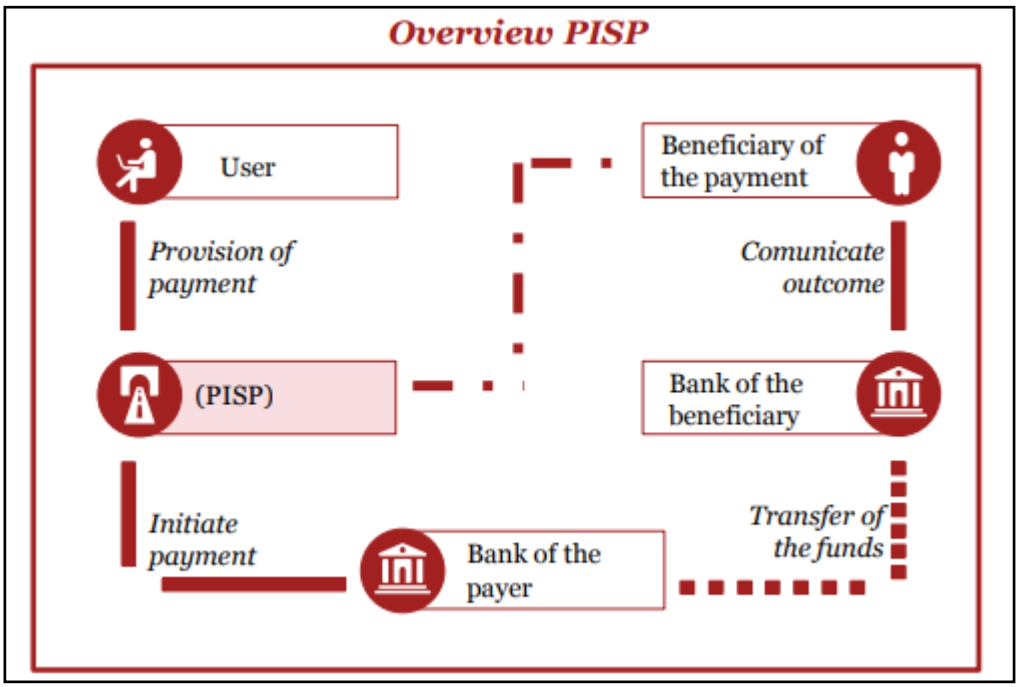

Image Source:https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf

Account Information Service Providers (AISP's) are the financial institutes that allow consumers and businesses to have a single window view on their financial situation. It enables the consumers to consolidate the different current accounts that they hold with multiple banks and to categories their spending according to different typologies (food, energy, rent, leisure, etc.), thus helping them with budgeting and financial planning with a single window dashboard access.

Responsibilities of Account Information Service Providers (AISP's):

- Initiation of retrieval of payment account information relevant to the payor by means of a third party provider application applicable to payment accounts accessible online.
- Explicit account holder's consent required by way of SCA.
- No dependence on a contractual relationship between AISP and account servicing payment service provider.

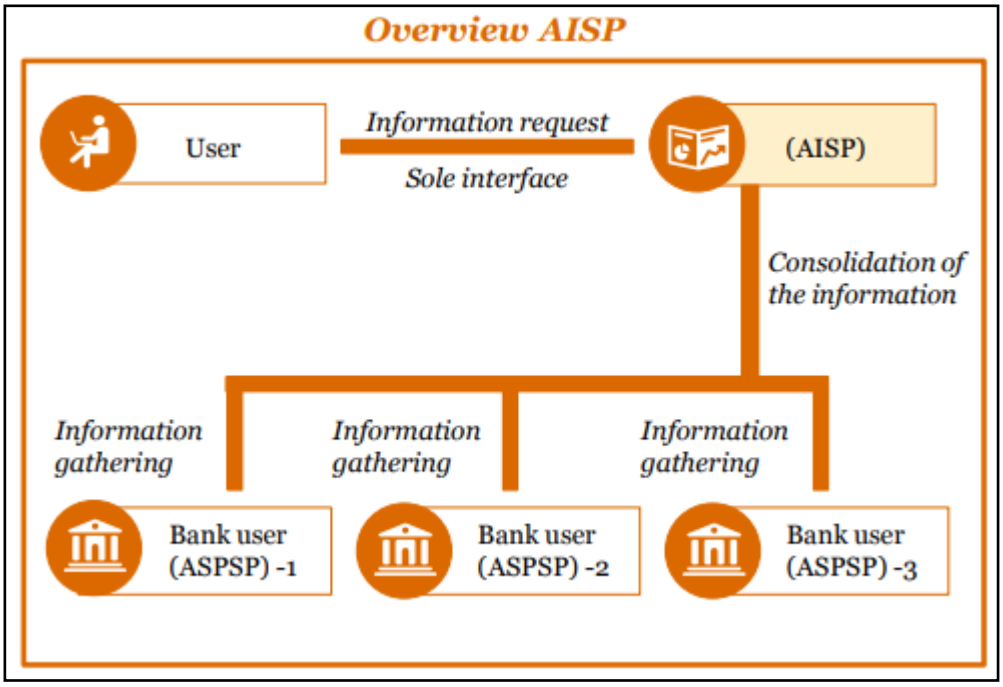

Image Source:https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf

Reporting Structure under PSD2:

PSD2 is a robust and future-oriented payments strategy that comes with lot of responsibility and reporting to regulatory authority, failing to which will not only attract penal charges as well major reputation loss for the bank. The Payment Services Regulations 2018 as transposed to national law by Central Bank of Ireland, place a number of reporting requirements on payment service providers (PSPs) and categorically establishes the the expectations of the Central Bank of Ireland in terms of PSPs meeting. These requirements are set out below. *(centralbank.ie/regulation/psd2-overview/psd2)*

- Major Incident Reporting
- Operational and Security Risk Reporting
- Payment Fraud Statistics Reporting
- Denial of Service Reporting

As per EBA , ***Major Incident Reporting*** is defined as per Regulation 119 of the Payment Services Regulations 2018 provides that, *"a singular event or a series of linked events unplanned by the payment service provider which has or will likely have an adverse impact on the integrity, availability, confidentiality, and/or authenticity of payment-related services."* The timeline of such reporting clearly classifies that PSPs need to submit an initial report of a major incident to the Central Bank within four hours from the moment the incident has been classified as *Major.* A comprehensive list of all such reporting criteria along with Risk categorization has been clearly specified in the website of the Central Bank of Ireland - referred as *National Competent Authority (NCA) as per EBA in PSD2.*

The incident classification exercise should be completed in a timely manner after the incident has been detected, but no later than 24 hours after detection. It is also classified by Central Bank of Ireland that if the PSP has not classified the incident classification within 4 hours of occurrence then the PSP to notify its supervisory team in the Central Bank, using phone or email channels, that an incident has occurred and is under review. There is specific template as provided by the Central Bank in its website consisting of three sections that the Central Bank

expects PSPs to populate until the conclusion of the incident. As per the guideline, the PSPs must submit their final report within a maximum of 20 working days after business starts functioning normally. The final report should contain detailed information along with root cause and actual figures on the impact of the incident to replace any potential estimates.

Operational and Security Risk Reporting as stated under Regulation 118 of PSR 2018 requires PSPs to provide to the Central Bank annually, an updated and comprehensive assessment as per the reporting template specified in the website of the Central Bank:

- Any Operational and Security Risk relating to the payment and services as provided by the PSP.
- Adequacy of the mitigation measures and control mechanism implemented in response to such risk that arises.

Payment Fraud Statistics Reporting guidelines as set by EBA clearly mentions the role and reporting responsibilities of the PSP's as effective from January 2019. PSP's must report statistical fraud data for all unauthorized payment transactions made and payment transactions made as a result of payor manipulation where a fraudster manipulates a payor to issue a payment order or give instruction to the PSP. The PSP's are supposed to do such reporting to the Central Bank semi-annually within timeline of 3 months after the end of reference period.

Denial of Service Reporting stated as per *Regulation 44(3) of PSR 2018*, any credit institutions must inform to the Central Bank of Ireland without any delay when an application for access to their payment account services by the PSP is rejected. *Regulation 92(9)* further stated that PSP's must inform CBI immediately after denying an AISP or PISP access to a payment account with adequate reason for such rejection. The Central Bank of Ireland has specified template of such reporting to be done by the PISP.

Benefits of Collaboration with FinTech companies-

To manage PSD2, it is recommended to consider partnering with some efficient and experienced FinTech firms having proper credential of all relevant processes and regulatory requirements, giving us the ability to focus on developing our customer service solutions rather than negotiating regulatory norms. Such Fintech firms will effectively integrate banking processes with the changing regulatory environment and ensure all guidelines and reporting's are done as per order. Some notable names in the domain of PSD2 are – *Figo AI & Salt Edge.*

Some of the key supports that a bank can leverage through such Reg-Tech collaboration are highlighted below.

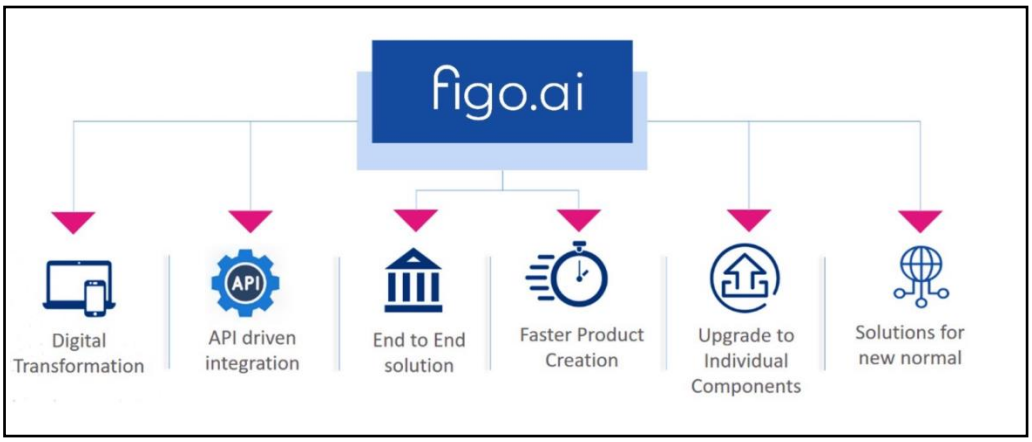

Image Source: Figo.ai

Figo AI, a German based Fintech firm, has mastered as a financial innovator with a modern cloud platform and democratizes access to financial innovation. Figo AI can augment our speed to acquire market share by ensuring to deliver the regulatory burden as well lower overall technology costs and resource level costs allowing us to focus and dedicate on our core banking solutions and customer services. Figo AI has dedicated solution to cater PSD2 with their new innovation – RegShield. This solution has focused approach towards PSD2 obligations and provides many of the authorization requirements including:

- PSD2-compliant customer processes to ensure 100% adherence of the regulatory guidelines.

- Regular internal audits checks and to prepare for external examinations.
- Setting up of proper governance and security policies viable for the bank.
- Managing the security incidents and ensure timely regulatory reporting
- Regulatory and compliance expertise
- Outsourcing controlling through SCA and control TPP access.
- Business continuity management

SaltEdge, a UK based corporate, is another Fintech company worth mentioning in the domain of PSD2. With over a decade of expertise, SaltEdge is a leader in consulting and complete open banking API solutions. SaltEdge offers full-stack toolkit specially designed for banks is Software as a Service (SaaS) based solution with all open banking requirements covered as required under PSD2, offering a cost-effective and technically scalable approach to compliance, requiring minimum technical involvement from the bank side. SaltEdge takes care of all the regulatory required components, ensuring a secure ecosystem.

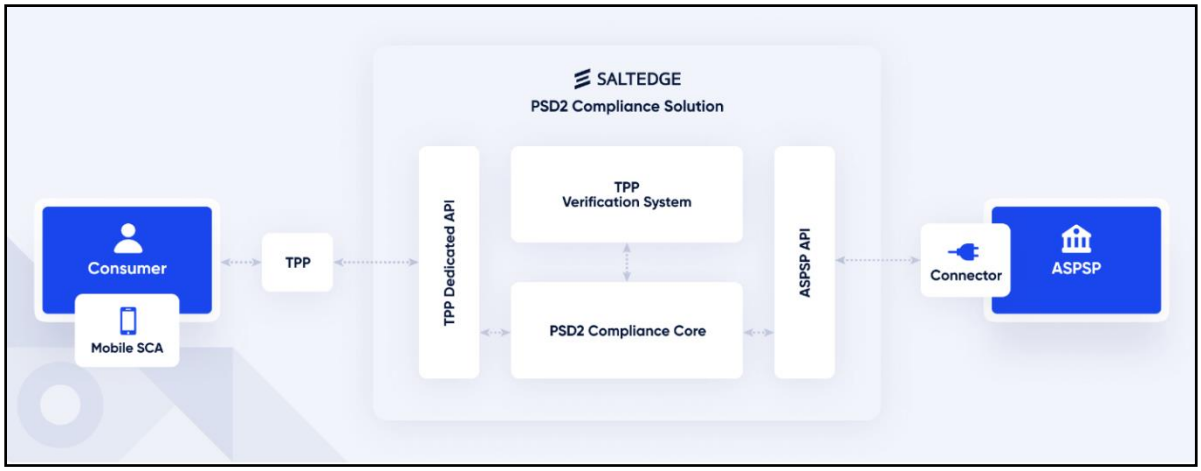

Image source: https://www.saltedge.com/products/psd2_compliance

Some of the key offerings that will be beneficial for the bank are –

- Comprehensive set of API's and ensure to meet the strict PSD2 requirements on Strong Customer Authentication (SCA).

- Dedicated environment for the TPP that includes an API access, ticketing system, monitoring dashboard.
- A comprehensive single window dashboard to see insights and monitor performance at-a-glance.
- TPP Verification system to filter out and authenticate the access and to know exactly who is connecting to the banks API and control such access within the regulatory framework.
- Mobile SCA solution for secure actions.

Conclusion:

Through this report, we have explored the various facets of PSD2, including its regulatory framework, security measures, the reporting structure, role and responsibility of the bank and its impact on the Irish financial landscape. We have also seen how *PSD2* was transposed into Irish law by *Statutory Instrument No. 6 of 2018, the European Union (Payment Services) Regulations 2018 (PSR)*, which became effective in Ireland on 13 January 2018. We have emphasized on role of TPP's in this eco system and various compliance under PSD2. I have highlighted in this report that focus of our bank will be to prioritize robust authentication mechanisms, secure communication channels and data protection protocols to ensure compliance and timely reporting under PSD2 requirements. For this purpose, the importance of collaborating with FinTech companies and benefits that can be leveraged has also been examined. By abiding and maintaining PSD2 compliance, will help the bank to foster resilience, innovation and trust in the dynamic realm of payment services in European Union.

References:

1. 'A Guide to the Payment Services Regulations in Ireland' Available at : https://www.dilloneustace.com/uploads/files/A-Guide-to-the-Payment-Services-Regulations-Aug-2019.pdf (Accessed on 5th Dec 2023)
2. 'Payment Service Directive' Available at: https://en.wikipedia.org/wiki/Payment_Services_Directive (Accessed on 5th Dec 2023)
3. Central Bank of Ireland – 'PSD2 - Reporting Requirements' Available at: https://www.centralbank.ie/regulation/psd2-overview/psd2 (Accessed on 22nd Dec 2023)
4. EY – 'Regulatory Agenda Updates' Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/bcm-pdf/ey-regulatory-agenda-updates.pdf (Accessed on 20th Dec 2023)
5. Figo AI 'We build digital banks and fintech solutions' Available at: https://figo.ai/ (Accessed on 01st Jan 2024)
6. PSD2 – 'Frequently Asked Questions' Available at: https://www.centralbank.ie/regulation/psd2-overview/faq (Accessed on 4th Dec 2023)
7. PWC 'Main regulatory changes introduced' Available at: https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf (Accessed on 22nd Dec 2023)
8. SaltEdge 'PSD2 compliance solution' Available at: https://www.saltedge.com/products/psd2_compliance (Accessed on 03rd Jan 2024)