Seven Pillars Institute
Moral Cents Vol. 6 Issue 1, Winter/Spring 2017

The Ethics and Financial Issues of PSD2: Demise of Banks and Other Risks

Genevieve Crawford

Abstract: The Revised Payment Services Directive or 'PSD2' will come in force in January 2018, extending the scope of the previous service direction by introducing third party access to accounts. The two new players are payment initiation service providers (PISP) and information services providers (AISP). These Third Party Providers can offer services in competition to existing banks and financial intermediaries, acting as software bridges between banks and merchants. This paper evaluates the financial and industry risks as well as ethical issues arising from PSD2.

Introducing PSD2

The Revised Payment Services Directive or 'PSD2' is a new legislation adopted by the European Union in 2016 (The European Parliament and the Council of the European Union, 2015). PSD2 extends the scope of the previous Payment Service Directive 'PSD' by introducing third party Access to Accounts (XS2A). It aims to prohibit surcharging and introduce strong customer authentication (SCA) for payments (24 Solutions, 2016). The PSD2 becomes enforceable on 13 January 2018. By this time, EU member states must publish national laws to conform. Likewise, financial institutions must revise their current IT networks to accommodate for PSD2 (Shahrokh Moinian, 2016). There are wide-reaching implications for banks, other PSPs, Fintech firms and customers.

The purpose of PSD2 is to drive competition and innovation by reducing barriers to entry for payment services. PSD2 widens the scope of the regulatory framework to include new players known as Third Party Providers (TPPs). In particular, the two main new market entrants will be payment initiation service

providers (PISP) and information services providers (AISP). A PISP is any organisation that initiates a payment with a software bridge between the merchants website and the online banking platform. An AISP is any provider that wishes to aggregate online information of one or more payment accounts and present it in a form of a single dashboard for the customer (Boden, 2015). By gaining access to customer accounts, TPP's can offer services in competition to the existing banks and financial intermediaries.

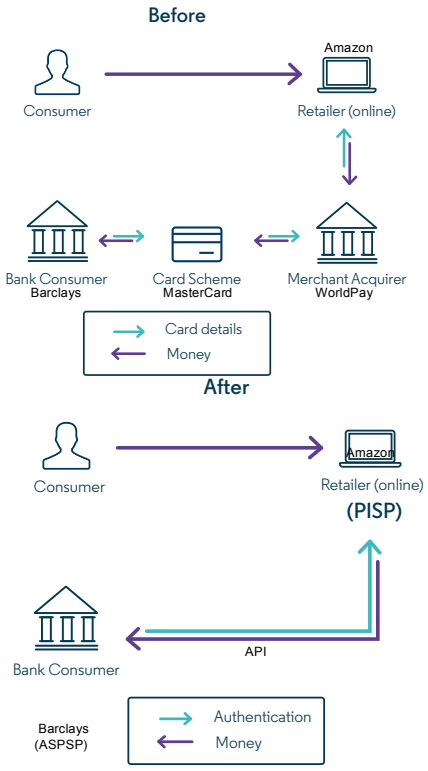
Readers are warned this article uses acronyms. The definitions table below serves as a guide.

PSD2	Revised Payment Service Directive is the new legislation adopted by the EU, enforceable on 13 January 2018. It is a revision of the first payment directive PSD. It also gives a legal framework for XS2A, API's, ASPSPs, PISP's and AISPs.
PSD	PSD is the first Payment Service Directive implemented in 2009 by the EU. It was introduced to establish a European-wide legal framework for payment services. It also introduced 'payment institutions' and defined them as providers of payment services, unconnected to the taking of deposits or issuing electronic money (Mastercard, Visa)
XS2A	Access to Accounts is part of the PSD2 legislation ensuring both financial institutions and non-financial market players may obtain access to the bank account of European customers
TPP	Third Party Providers are third parties alongside banks and customers in the payment process. TPP is a broad term for companies that are PISP's and AISP's.
PISP	Payment Initiation Service Provider is any organisation that initiates a payment with a software bridge between the merchants website and the online banking platform. (Amazon, Sofort, Trustly)
AISP	Account Information Service Provider is any online provider that wishes to aggregate online information of one or more payment accounts and present it in a form of a single dashboard for the customer. (Mint.com)
ASPSP	Account Servicing Payment Service Provider is a financial institution that will be obliged to open up an API to allow TPP's to initiate payments and access account information. (Banks - Barclays)
API	Application Programme Interface is a set of commands, functions and protocols programmers can utilize when constructing software for an operating system. It is the software network that banks will use to send and receive payments. Open API's are designed to be easily accessible by the general population. In 2018, any person outside the organisation can register for access to the API.
EBA	European Banking Authority is a regulatory agency of the EU.
SCA	Strong Customer Authentication is a two factor authentication that requires a clarification of two of the following: something you know (e.g. username, password), something you possess (mobile phone, card or authentication code generating service) and something you are (fingerprints, voice recognition)
TLS	Transport Layer Security is a cryptographic protocol that provides communications security over a network.
DoS	A Denial of Service attack is a cyber-attack where the perpetrator seeks to make a network unavailable by disrupting the host's connection to the internet.

PSD2 is designed to regulate online shopping without the need for a credit or debit card. As approximately 60% of the EU population does not have a credit card, TPPs will open up markets and offer financial services to those who are

currently excluded. Furthermore, PSD2 bans card surcharges in the vast majority of cases to help lower charges for EU consumers (24 Solutions, 2016). As estimated by payments UK, consumers are predicted to save 730 million euros on card transactions per year (European Commission, 2015). With new security measures in place, consumers will be better protected against fraud and other payment abuse incidents (European Commission, 2015). On the other hand, the issues resulting from PSD2 include network cyber attacks and misuse of customer information by AISP's. While the EBA promises security, there are still potential issues on a firm level. Consumers may become more exposed to cyber hacking and be more vulnerable to act on misleading economic inferences due to mistrust by artificial intelligence. Although the purpose for PSD2 is to foster innovation and reduce barriers to entry, the potential impacts on consumer safety are an issue banks and financial institutions must help mitigate throughout the transitional period.

How PSD2 Works



To explain how PSD2 works, say a customer is shopping online at Amazon. Today, the customer buys an item by entering in her debit card details. Amazon contacts the merchant acquirer (e.g. WorldPay) who further contacts the customer's card scheme (e.g. MasterCard), who then withdraws money from the customer's bank (e.g. Barclays). In January 2018, after the PSD2 is enforced, the customer will purchase an item but Amazon takes her to a portal where a Payment Initiation Service Providers (PISPs) requests permission to withdraw the amount from an Account Servicing Payment Service Provider (ASPSP). In this case, the customer's bank account at Barclays is the ASPSP and Amazon is the PISP. Once the customer enters in her bank login, the PISP contacts Barclay's via an open Application Programme interface (API) to process the payment instantly. There are no additional transaction costs. This is similar to the way sites are able to access Facebook accounts today. Next time the customer shops at Amazon; permission to access her account will remain active until, for whatever reason, it is revoked (Boden, 2015).

The Effects of PISP Emergence

Indeed, the previous example does not seem much different to the current situation of online payment services from the perspective of customers, as the PISP is the merchant itself. However, in the next 12 months many online companies will not be able to develop the API technological infrastructure to acquire authorisation from the EU to become PISP's in time for the directive launch. To become a PISP, a company must be licensed by the competent authority and have an initial and minimum ongoing capital of 50,000 euros (Shahrokh Moinian, 2016). Thus, many small businesses will rely on an outside source to control the payment between them and the bank. While PISP's already exist in Europe in the form of companies such as Sofort or Trustly, PSD2 will create a whole new field of market entrants to initiate payments between the merchant and the bank (PWC, 2016). This also allows companies such as Google Wallet or Apple Pay to become PISP's, hence combining the ASPSP and PISP aspect (Evry, 2016).

Banking is necessary; banks are not.

(Bill Gates, 1990)

Access to Accounts (AX2A) is an element of PSD2 that ensures if the customer gives consent, TPPs may obtain access to bank accounts via banks open API's (Boden, 2015). This will enable TPP's to build financial services on top of banks' data and infrastructure. The banking sector's monopoly on its customers' account information and payment services will cease to exist. As new players come into the market, banks will find it difficult to differentiate themselves from Fintech firms in the loans market. This is because the new players may access to the same information that banks have, and could offer loan services at a lower price. Financial institutions will not be competing with other banks but rather, the whole Fintech industry in general. One may even question whether banks will need to exist in the future. Hence, PSD2 imposes substantial economic challenges and costs for banks and financial institutions alike. A former reliance on companies such as Visa and Mastercard will decline. It will cost banks vast amounts for IT services to construct their open API's before 2018. While banks fight to maintain market share, it is predicted that up to 43% of bank revenues will be lost to PISP services by 2020 (Services, 2016). These revenues are currently in the form of transaction costs and card surcharges. During the transitional period of establishing the PSD2, banks must acknowledge such a future climate in the best interest of their depositors and creditors. As many may be burdened with financial difficulties in the future, banks must start acting prudently to prepare for what is to come.

Security of PISP's

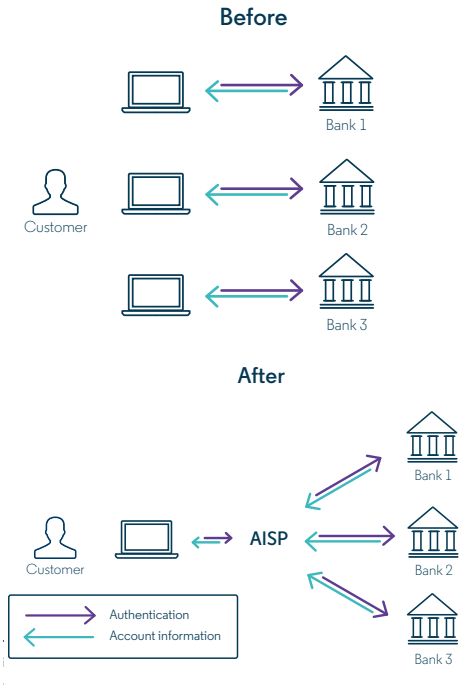
In August 2016, the European Banking Authority (EBA) published their draft regulatory standards for strong customer authentication (SCA) and secured communication under the PSD2 (EBA, 2016). Customers will have to adhere with SCA when a payment is initiated. SCA under the PSD2 is a two-factor authentication that requires a clarification of two of the following: something you know (e.g. username, password), something you possess (mobile phone, card or authentication code generating service) and something you are (fingerprints, voice recognition) (24 Solutions, 2016). As opposed to the current system where a card only requires a signature or a simple swipe, this is a vast improvement for security. The EC has stated that due to improved harmonisation of liability rules in unauthorised transactions, the maximum amount a payer could be obliged to pay will be decreased. The potential amount payable by the depositor for an unauthorised transaction will now be 50 euros, as opposed to the previous amount of 150 euros (European Comission, 2015). In the event of an unauthorised, non-executed or defective payment withdrawal initiated via the PISP, the ASPSP is required to refund the customer immediately. If the company who initiated a false withdrawal via a PISP is liable for the payment, there is an obligation for the company to immediately compensate the ASPSP. Of course, this is unless the PISP can prove the transaction was actually legitimate (EBA, 2016). While this new liability regime aims to compensate the consumer regardless, there is a lack of clarity between the PISP and ASPSP in the event of loss. In other words, while payment authentication is improved by PSD2, payment disputes are inevitable and will continue to be a complication for APSP's and PISP's alike.

A main issue regarding the enforcement of PSD2 is the security of customer payments. There have been criticisms from technical experts on the system. First, banks must train their IT systems to cope with potential cyber attacks. Traditionally, a Transport Layer Security (TLS) is used to secure a connection between two points. While API's will be designed to run using TLS to secure connections, the use of such software comes with potential difficulties. If an API disables a request made to take a payment from an account, the request can be re-sent through a standard browser demand. This introduces vulnerability for the API; it may be tricked into accepting a request thinking it is secure. That is, in the event of the TLS not functioning properly. Furthermore, a Denial of Services (DoS) can prevent a bank's API from working. Once the Internet connection is re-established after a DoS, the amount of sheer traffic as a result of the DoS could lead to an API's inability to filter insecure requests. To eliminate cyber attacks from hackers there needs to be robust authentication barriers. In terms of the merchant, there needs to be a concrete clarification that the PISP is who she says

she is. In terms of the customer, there must be confirmation that she purchased the goods. This requires an SSL certificate to be validated. Again, the validation process does not come without difficulties. If exploited, a hacker can fake an SSL certificate to obtain the customer's username, password and account information (Mytton, 2016).

From a technological point of view, the introduction of API's for banking systems are threatened by cyber criminal activity. One can argue that although the PSD2 aims to enhance innovation, its removal of traditional payment authentication potentially exposes bank depositors to large losses due to the bank's negligence. These losses encompass not just monetary values, but also potential theft of identity. The economic effects of such a large-scale cyber attack would be catastrophic, spanning from huge losses to crippling bank runs. As a result, banks must consistently audit their API connection, particularly during the transitional period of the directive where banks are most vulnerable to cyber attacks.

The Effects of AISP's Emergence



An Account Information Service Provider (AISP's) collects information from a consumer who has numerous bank accounts and consolidates it in one single place. As previously mentioned, the AX2A segment of the legislation now allows companies to see bank account information with the consent of the customer. Under PSD2, AISPs will be able to get insightful views on a person's financial situation and make economic inferences about her income and expenses. This means new Fintech companies can see what type of spender an individual is, what products are trending and offer financial consulting and management. While AISP services exist today in the form of companies such as Mint.com, the PSD2 is a huge step in the Fintech movement as it enables a person's transaction history to be accessed without customers surrendering their passwords (Boden, 2015). Since consent is gained by AISP's from a simple click of a button, customers may give access to account information without realising potential consequences. As this feature of PSD2 can be utilized by companies in many ways, Fintech firms acting as AISP may seize the opportunity to offer services that are not in the best interests of their clients. Consequently, Fintech firms are able to exploit future customers to make profits

or engage in criminal activity. Consumers must become aware of the potential detrimental outcomes of releasing their information to AISP's.

Ethical Issues of AISP's

At this stage Fintech firms by their nature have little reputation at stake. In comparison to banks, they have no deposit liabilities or central bank supervision. To become an AISP, there is no requirement for any initial capital or company funds (Shahrokh Moinian, 2016). Due to the way they are established, Fintech firms using AISP's generally will not have much skin in the game once the PSD2 comes into place. They will be susceptible to taking riskier business strategies. If the company providing the information has all the power to make inferences about the customer's financial position, the AISP is in a position to offer advice. While this may be seen as a beneficial financial service, it may not be in the best interest of the customer but rather, assist the AISP firm in increasing profits. Take for instance, a person with limited investment knowledge allowing an AISP to access her account information. The AISP consolidates the client's banking statements, gives an extensive overview of the current market trends and offers her investment suggestions. This advice is to invest in a stock which, incidentally, the AISP firm owns as well. By driving up the stock price, the firm gains a profit simultaneously. Or alternatively, consider an AISP firm convincing a client to invest in a private company involved in criminal activity. The ethical ramifications and adverse outcomes are significant. The EU must watch carefully to determine whether Fintech companies provide information in the best interest of their customers. Meanwhile, customers must be educated on the potential risks they take on by allowing an AISP to access their account.

PSD2 is a unique legislation in that it fosters financial development. From an ethics standpoint, it is most important to reflect on who may be taken advantage of in the soon-to-be situation. From the consumers' point of view, there are obvious gains from the introduction of PSD2. These can be summarised as a decrease in card surcharges and an increase in authentication security, at least theoretically. The emergence of TPP's will result in financial inclusion for many people in the EU who do not have credit cards. On the downside, there is a lack of clarity between PISPs and ASPSPs in the event of loss. With cyber attacks, the obligation of repayment is difficult to assign. While emergence of AISP services is beneficial for consumers to consolidate their financial position, they do not come without risks. Customers are vulnerable to misleading financial information and must be cautious about the entities which they authorise to view their account histories. The EU must monitor such activities of Fintech firms in the years to come.

Banks should act swiftly with their API infrastructure development to establish the necessary payment platforms before 2018. Once PSD2 is introduced in Europe, banks interest revenue stream and information monopoly will be jeopardised. The way banks manage this will be crucial for investors and depositors alike. If banks are unable to develop sound API infrastructure to become reliable ASPSP's, their market share will be lost to Fintech firms. Accordingly, if the API infrastructure offered by banks is not robust, depositors are vulnerable to cyber attacks. Banks must consistently monitor and audit their API network to decrease the chance of this happening. By their mere nature, Fintech firms - new PISP's and AISPs - have little reputation at stake. This means they may be inclined to take riskier business decisions, or even involve themselves in deceptive business activities. Customers must be aware of this before they seek financial advice. While PSD2 is considered 'the biggest technological innovation in retail banking since the Internet', the EC and EBA must address potential risks without stifling innovation (Boden, 2015).

-x-

Bibliography

24 Solutions. (2016). *Smedjegatan 2c | SE-131 54 Nacka | Sweden | +46 (0)8 535 24 100 | www.24solutions.com PSD2—What are the implications, problems, possibilities, challenges and opportunities*. Retrieved December 15, 2016, from https://www.24solutions.com/en/wp-content/uploads/sites/3/2016/11/24S_PSD2_Whitepaper.pdf

Boden, A. (2015, October 9). *Explaining PSD2 without TLAs is tough!* Retrieved December 14, 2016, from Starling Bank: https://www.starlingbank.com/explaining-psd2-without-tlas-tough/

EBA. (2016, August). *CP ON DRAFT RTS ON AUTHENTICATION AND COMMUNICATION UNDER PS D2*. Retrieved December 17, 2016 , from Eurpoean Banking Authority: https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf

European Commission. (2015, October). *Payment Services Directive: frequently asked questions*. Retrieved 2016, from European Commission : http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

Evry. (2016). *PSD2 - Strategic Opportunities beyond compliance*. Retrieved December 13, 2016, from Evry: https://www.evry.com/globalassets/bransjer/financial-services/bank2020/wp_psd2/psd2_whitepaper.pdf

Mytton, S. S. (2016, November 11). *Preparing for PSD2 – How banks and retailers are approaching the five big issues around APIs*. Retrieved December 8, 2016, from IT Pro Portal: http://www.itproportal.com/features/preparing-for-psd2-how-banks-and-retailers-are-approaching-the-five-big-issues-around-apis/ pwc. (2016).

PSD2 in a nutshell. Retrieved December 13, 2016, from PWC: https://www.pwc.com/cz/en/bankovnictvi/assets/psd2-nutshell-n01-en.pdf Services, A. P. (2016). *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive*. Retrieved December 17, 2016, from https://www.accenture.com/t20160505T180127__w__/ca-fr/_acnmedia/PDF-

15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive%20%281%29%20%281%29.pdf

Shahrokh Moinian, D. H. (2016, September). *Payment Service Directive 2*. Retrieved December 17, 2017, from Deutsche Bank AG: http://www.gtb.db.com/docs_new/White_Paper_Payments_Services_Directive_2.pdf

The European Parliament and the Council of the European Union. (2015, November 25). DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Offical Journal of the European Union* .