Open banking's PSD2:

Open trust v Open abuse

LYSIS FINANCIAL
Expert Governance, Risk & Compliance Consulting

Written by James Emin

London:
6th Floor
125 Old Broad Street
London, EC2N 1AR,
United Kingdom
Tel: +44 845 658 0008

New York:
19 W34th Street,
Suite 1018,
New York, NY 10001,
USA
Tel: +1 646 828 8264

Frankfurt:
1st Floor, An der Welle 4,
Frankfurt am Main
60322,
Germany
Tel: +49 69 75938410

Edinburgh:
9-10 St. Andrew Square,
Edinburgh,
EH2 2AF,
United Kingdom
Tel: +44 131 281 2131

Dublin:
Ground Floor,
One Georges Quay
Plaza,
Dublin 2, Eire
Tel: +353 1 9073297

Paris:
Club Buro Vendome,
5 Rue de Castiglion,
75001,
Paris, France
Tel: +331 5345 1063

For more information please contact us at: info@lysisfinancial.com

Contents

1. OPEN OPPORTUNITY

1.1 IN A NUTSHELL

Open banking is what it says on the tin. It empowers retail consumers and SMEs within the EU to have open access to their bank accounts through FinTechs intermediary functionality, then takes control of their current account data to view or initiate payments permitted via registered or regulated TTPs (Third Party Providers). Enabling consumers to be better informed of what products and services outside the offering of their traditional banking relationships.
The 2 primary TPPs are:

- AISP (Account Information Service Providers) An app that can aggregate many payment accounts data
- PISP (Payment Initiation Service Providers) Assesses and initiates payments from payment accounts

Both require customers explicit consent by SCA (Strong Customer Authentication) that identifies and verifies customers digitally, using the banks secure login credential's i.e. password /code, biometric or text confirmation to validate.

In the context of PSD2, Banks / Building societies are:

- ASPSP (Account Service Payment Service Providers) i.e. retail banks, be it traditional / incumbent or challenger/ neo

1.2 BACKGROUND

The concept of Open banking, specifically to the UK is nothing new and was triggered back in November 2014, by a CMA (Competition and Markets Authority) investigation, which explored greater competition within retail banks (incumbents) that finalised with a report in August 2016. The primary recommendations of the final report was to increase competition within the retail banking sector by setting out key requirements for retail banks to expose their customers transactional data with third parties that would deliver retail banking services at a competitive rate. Running in parallel, the European commission started

their 2nd review of PSD2 (Payments Services Directive 2) that also set out requirements for pan European competition, by mandating retail banks to open up customers data with customers consent with the main aim to enhance regulation and harmonisation.

A report in June 2019 by the OBIE (Open Banking Implementation Entity) has forecasted that the UK retail banking population could gain £12 billion a year through this initiative, with businesses realising a further £6 billion in value. People could save as much as £287 per year, 2.5% of their annual income if government, regulators and industry can work together to:

- Deliver greater value for consumers: By increasing competition and consumer data transparency
- Build a trustworthy ecosystem: Consumer protection and rights, built on obligations from payment providers
- Stimulate the market to action quicker: By incentivising Fintech start-ups with financial rewards of funding.

The above objectives are to afford retail consumers greater choice to obtain this value. This has led to an insurgent surge in Fintech start-ups, neo and challenger banks many that have come up with quirky and creative apps to ethically exploit PSD2 and rapidly build up a subscription base, by making it easier to move, manage and make money for their customer base. This has already radically changed the way in which customers engage with financial services.

We live in an era where a majority of 'banked' individuals are smart phone co-dependent. Using apps that have transformed the way we manage our lives that has led consumers expecting nothing less than a swift, seamless and intuitive user experience, which gives the consumer the wow factor. This should undoubtedly make managing personal finances fun by providing an aggregated overview of their spending habits with the hope of taking away the taboo of discussing money concerns with family, friends and peers. Since PSD2 came into force on the 13th January 2018, a financial technological ecosystem has evolved where Fintech and incumbent banking apps integrate in this eco systems via APIs or screen scrapping –apparently soon to be outlawed. Traditional banking business models are under threat as there could be demise in maintaining client facing relationships to offer services and products. Bank accounts maybe simply used as a utility and custodian of clients' money.

Fintech and incumbents are already working collaboratively at a global level and national level. The UK has set up an organisation called Open banking limited (now called OBIE) that was funded by the big 9 banks and

backed by UK Government. To explore how industry best practices and standards could be consistent derived primarily from EU commissions PSD2 RTS (Regulatory Technical Standards). While this may seem within confines of Europe, Open banking has become a global phenomenon. Innovators are already democratising the financial system as we know it by disintermediating the banking system. Creating ways to facilitate the transfer of currency cross border with competitive exchange rates, in real-time at little cost while maintaining the intrinsic trust of both settlor and benefactor that the funds get to their destination without incurring additional opaque fees or surcharges. Furthermore, a 24-7 service offering is allowing customers and corporates to send, receive the track payments in real-time from their UK bank account, enabling customers to track as see exactly where their payments have been made and received in the network, using software-as-a-service (SaaS).

2. OPEN THREATS

Considering an incumbent's first line of defence model, whereby traditional banks relationship managers maintain that relationship of knowing their clients and their clients business, which is a vital barrier to prevent and deter fraud and financial crime. Could this Open banking money revolution plus the demise of front office relationships; open up risk of abuse that could allow nefarious actors to form innovative sophisticated schemes, within this radical transformation and democratisation of financial services.

From cybercrime and fraud, unauthorised and unethical data use that breach GDPR and even more sinister identity theft. Through to facilitating the concealment and movement of the proceeds of crime, this would also include the scope of tax evasion, bribery and corruption, terrorist finance through to export control and sanctions circumvention. Open banking is slowly fragmenting the silos that have traditionally mitigated both fraud and financial crime.

2.1 CYBERCRIME

PSD2 stipulates that registered (via national financial regulator) TTPs must be trusted by banks to provide clients data (with customer's explicit content) while on paper this may be seamless; there are ongoing concerns of trust, RTS's (regulatory technical standards) are neither regulatory, technical or standard meaning no 2 European banks may not the same in terms of inoperability API. In the UK you have the 'OBIE standard' in France you have 'STET' and pan European has 'Berlin Group'. Therefore, each TPP will have to do something different with each European bank. This could lead to customers trying to determine what the

trusted norm is and more challenging how can banks demonstrate a TPP can be trusted given the complexities of mapping different EU jurisdictions, levels of regulations and registration. Currently banks cannot block screen- scraping, however they could refuse to refund fraud loses if customers choose to share login details with a firm that isn't authorised and regulated, that-said, how can this fraud be prove the fault is that of the bank or customer?

While screen-scraping is still in use, in which the third party imitates a user and goes via the consumer login. Meaning they need to know the consumers login credentials in full and be able to use it in an unencrypted form. Could customers data be unscrupulously provided by unwitting participates within the eco systems, or could client's data be extracted and sold on to uncompliant (GDPR) marketers or at worse cybercriminals for use in identity theft. There is an inherent danger that replicated websites or apps open source platforms could mock TTPs who pose as a third party in correspondence to elicit information, which can allow cybercriminals to phish for client details, spoofing data subjects / customers into giving approval to access account information. This information could then be used to deceive customers into providing secure data.

2.2 GDPR

There has been debate to determine if GDPR and PSD2 are contradictory or complimentary?

2.2.1 CONTRADICTORY

When a data subject / PSU (payment service user) provides explicit consent for a TTP to access their personal data, there could be other data subject's data to consider, known as a silent parties data. This is where some other person transacts with consenters bank account, like reimbursing for a joint event (dinner Cinema etc.) The silent party has not consented to sharing their data with a TPP. This was a main topic of concern of many payment providers at the 2018 DPWF (Data Protection World Forum). The EDPB (European Data Protection Board) have confirmed in a letter to a MEP Sophie in't Veld a TTP may not require the consent of silent parties to process their data. "A lawful basis for the processing of these silent party data by PISPs or AISPs – in the context of payment and account services under PSD2 – could be the legitimate interest of a controller or a third party ... to perform the contract with the service user,"

Automated processing of personal data leads to profiling with the purpose of assessing personal features. Fintech and banks are growingly using AI automation to ensure a prompt, rapid and a decisive service at a cost effective rate, such as credit scoring. They are also vital real-time tools in combating fraud and money laundering. This seems to conflict with GDPR. Under article 22 of GDPR, 'the data subject shall have the right

not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Therefore firms must be able to explain every automated decision if requested by a data subject .With a legitimate rationale like explicit consent or a compliance and legal obligation (money laundering). GDPR does not infringe on innovation as long as data is processed in an ethical manor and can be adequately justified.

2.2.2 COMPLIMENTARY

Both pan European regulations (PSD2/GDPR) drive to customers to gain control of their own personal data as well as keeping it safe and secure. Article 94 of PSD2 requires all PSP (payment service providers), which includes PISPs and AISPs, to obtain "the explicit consent of the payment service user" in order to "access, process and retain personal data necessary for the provision of their payment services".

Data policies and practices should be led by more carrot and less stick from regulators, the carrot represents customer trust. FinTechs and InsurTechs are already ethically exploit data to better understand their customers that could provide better, bespoke and relevant products and services that are tailored around the customer's financial circumstances. Building trusts that demonstrating fraud prevention or how their personal data can by optimised to benefit them, rather than an organisation in which they entrust one of their vital asset – their personal data. PSD2 satisfies GDPRs data portably principle, though there are the challenges of how both parties (Bank and TPPS) can depict sensitive data from transactional payment accounts. For example if a data subject is a fee paying member of trade union or religious group that that data is classified as sensitives data, that will require firms to carry out a (DPIA) Data Protection Impact Assessment.

The global awareness via adverse media reports and documentaries of data misuse has increased data subjects to becoming acute on complex privacy policies and T&C's. Therefore clear transparency is critical in restoring trust with any tech company. In reality it's how a tech company behaves in the capacity of a data controller, explaining why and how customer's data is being processed and who it is shared with. Although GDPR stipulates that this must be communicated in a clear, concise and unambiguous manner. This proactive act of simplified transparency and control of consent will only build trust and trust leads to loyalty, which is the ultimate carrot for any Fintech start up.

2.2.3 DUAL REGULATION

GDPR is principles based, in February 2019, the ICO (Information Commissioner's Office), with the FCA (Financial Conduct Authority), issued a statement that it had signed an updated MoU (Memorandum of Understanding). The MoU sets out the principles of coordination and cooperation between two regulators and the legal framework that governs the sharing of relevant information and intelligence. This framework is built on collaboration and information sharing between the two organisations to discuss matters of interest in relation to FCA-authorised firms, certified individuals and approved persons of interest, which consults on any issues with significant matters of concern for both parties. This lawful exchange of information covers the purpose of the ICO discharging its function, the information that would be shared includes:

- Activity that could bring doubt on the fitness or propriety of a party that suggests there may be a failure of a firm's or persons regulated activities
- Any investigations and or action taken against a person or a firm; including criminal or civil proceedings

Both PSD2 and GDPR require incident reporting. It would be cognisant to consolidate one process that takes account of all of the possible recording, reporting and notification requirements to PSUs, ICO and FCA.

2.3 FINANCIAL CRIME

As previously stated the erosion of customer relationship with incumbent banks has demised that a single point of access that will take away the human oversight of 1stLoD. That in itself presents concerning challenging for senior managers who have to attest that they can demonstrate that have sufficient oversight and supervision to implement mechanisms to know and understand their customers. Through to monitor and control payment transactions. This could undermine or by pass fraud and compliance provisions banks place to detect potential wrongdoing early without alerting criminals to their presence. Banks can not been seen to put impediments on PSD2 core innovation objective, but equally when their in-house business model is Open to other participants this raises the question of regulatory reliance, that is a form of trust.

2.4 RELIANCE

In the wake of many DPAs (deferred prosecution agreements), many tier 1 banks undertook KYC programs to remediate their corresponding banking network, as the reliance of being just regulated was not reliable anymore. The due diligence requirements became more in-depth that went as far site visitations to review

then gauge their corresponding banking partners AML policies, KYC procedures and their over client risk demographic. In short this extended a new acronym, KYC-C Know Your Client's Client, which provides assurances to certified senior managers who have the burden of personal and criminal liability. They had to be confident of the funds flow conduit in which they are accountable for and ultimately oversaw and monitored had sufficient controls. As the Open banking eco system matures it they're going to see similar practices, instead of site visitation will there be a digital mechanism to provide assurance if and when the regulatory demand grow?

2.5 MODERN SLAVERY

FinTechs, TPPs and challenger banks are primary focused the on UX (user experience) which has seen the rapid growth of real time on boarding take place for many of the challenge banks, that take away the need to pop into a branch. Instead this is all being done on a smartphone marking the fact that accounts 'take minutes' to open. Real time on boarding / ID&V, utilises scanned / photo of ID documentation (passports, driver's license, utility bill etc) then validates that data in the backend by correlating the prospect customer's information with credit agencies or electoral role. They then use AI biometric facial recognition to match the phone pic verses ID pic which makes the process seamless. However, with the ongoing raise of modern slavery there is a risk that vulnerable individuals could be coerced into using their identity. Bank branch personnel are provided with training to spot such abusive and coercive behaviour, which would be difficult to detect virtually.

2.6 5AMLD AND CRYPTO ASSETS

Outside of the supervised financial network, cryptocurrencies are being exchanged via online exchanges. Cryptocurrencies price / rates have been volatile as the value is purely driven by market demand that is not backed by any central banks that are intrusted by governments and public to ensure monetary stability. Cryptocurrencies leave a traceable footprint of their source, but some ownership remains anonymised. Criminals can break the traceable audit trail by combining identifiable and anonymous funds together – this is known as 'tumbling'. As part of a broader service offering, some Open banking FinTechs have started to partner with cryptocurrency custodian wallet providers and cryptocurrency exchanges. The 5MLDs has expanded the EU's regulatory perimeter for controls that has bought into scope custodian wallet providers and providers of exchange services between virtual currencies and fiat currencies. When the 5thAMLD comes into force on 10th January 2020, both cryptocurrency exchange and cryptocurrency custodian wallet

providers will become an 'obliged entity' as defined under 4thAMLD which means they will be obligated to perform KYC, transaction motoring and submit SARs (suspicious activity reports).

3. OPEN STRENGTHS

3.1 REGULATORY ROADMAP

It's not all doom and gloom, there is a silver lining to the above mentioned threats one of the main control objectives of PSD2 is SCA (Stronger Customers Authentication) and CSC (Common and Secure Communication). The PSD2 SCA and CSC RTS requirements was due come into force in 14th September 2019.

SCA: To allow frictionless flow via 2 factor authentications a requirement for all electronic payments and remote access verification. This is authentication based on the use of two or more elements categorised as:

- Knowledge (something only the user knows i.e. password / code)
- Possession (something only the user possesses i.e. phone and key generation device)
- Inherence (something the user is i.e. fascial and voice recognition or thumb print)

The premise behind SCA 2 factor authentications is completely warranted – face to face card fraud was dramatically reduced with the introduction of the chip and PIN, a non-virtual form of SCA. Unfortunately chip and pin cannot be used in ecommerce that has led to a huge rise in online fraud. Unless you are an identical twin, biometrics should be difficult to circumvent, but also the most seamless to use, furthermore will also act as a deterrent to money launders. If they are unwilling to share their biometric data without a clear justification then this should be raised as a red flag in the on boarding process. With biometrics, bank can monitor patterns of behaviour and raise red flags if deviation from a norm happens.

It must be noted; the EBA's has recently provided discretion to national regulators as to delay SCA by 14th September, to which many have accepted. The primary reason for this flexible deadline is the card payment and merchant industry is simply not prepared and could lead to a significant impact on ecommerce.

CSC: Under the Common and Secure Communication RTS, ASPSPs are obliged by the CSC RTS to make their PSD2 interfaces in such a way that TPPs can identify themselves towards a bank. ASPSP must provide AISP's / PISP's a secure communication channel in order for them to access the payment account using APIs the API must allow TPPs to provide payment initiation or account information without unnecessary hindrance.

3.2 SCREENS SCRAPING

There is the argument to determine if screen scraping will be outlawed, a method to make automated use of a website is by acting like web browser to perform activities on that website that are usually manually performed by a user. It allows multiple user interfaces for the end user to aggregate data from multiple bank accounts, than from original web browser. If and when an ASPSP are providing a dedicated interface to AISPs and PISPs it may limit access to its account of the dedicated interface only if it is able to prove to have met all regulatory requirements. If these requirements are not met, the ASPSP has to allow screen scraping as a fall back option. Under Common and Secure Communication RTS AISPs and PISPs need to identify themselves regarding the ASPSP, they may not impersonate the PSU but in order to identify them will need to use eIDAS certificates to demonstrate compliance.

3.3 API'S

In terms Common and Secure Communication, API's are far more superior to screen scrapping. This network of API's constructs a trusted architecture. Think of API's as electric plugs that feeds data safely and securely between TTPs and bank / ASPSP. As previously mentioned, currently there are different EU API standards (plugs) that may require adaptors to ensure seamless interoperability. The robustness of API's is forcing hackers to find other tactics to penetrate the front door. The EU Commission accepts the challenges and concerns that there is a need to provide more granular requirements, but that obligation should be on market participants to collaborate in establishing solutions that works for all parties. To address these challenges the Commission has taken the lead in recommending the formation of an API EG (Application Programming Interface Evaluation Group) to evaluate and assess standardised APIs specifications to assist in ensuring that the compliance needs of ASPSPs, TPPs and PSU are met within scope of PSD2 and GDPR. The EU Commission, the EBA (European Banking Authority), and ECB (European Central Bank) will act in the capacity as observers in the API EG, therefore will provide ad hoc assistance to market participants. Whether the Open banking industry will be converging to a global API standard, remains to be seen.

3.4 FCA SANDBOX

When the FCA was formed in 2013, it extended its regulatory powers to include competition, addressing some problems consumers faced in markets. Competition was the key driver in tackling these issues and

innovation was keys. The FCA foresaw that many tech innovators where not from the traditional financial services background and would be concerned at how they would navigate around the costly regulatory red tape. Therefore the FCA set out an approach to ensure the tech innovators journey with them was easy and friendly. Project Innovate (now called Innovate) was conceived by simplifying the application and authorisation process that established could a firm and their business case and model be trusted by falling within rules that also protected consumers. The benefit for firms was reduced time-to-market and gain better access to finance. Innovate was a call for firms to come forward so that the FCA could help support them with their journey in getting their products and services to the market as a competitor, ensuring that appropriate consumer protection safeguards where build it. The clear objective that had to be satisfied was reducing costs to consumers. Given this regulatory initiative was the world's first, a safe and controlled environment to test these products and services was needed. Therefore, the FCA Sandbox was formed for a small scale testing with a limited number of customers, with test periods of around 6 month where both the FCA and the firm could mutually learn. Subsequently after the test period the firm would have a decision to make commercially; either take to the market permanently and remain authorised (meeting FCAs criteria) or exit with a plan in place to limit an impact to consumers. Think of Sandbox as a clinical trial in safe environment before going mass market. With these proofs of concepts being recognised by a world leading authority (FCA), has now helped start-ups gain traction and trust that has led to greater access of further rounds of VC funding.

4. THE FUTURE IS BRIGHT

4.1 REG TECH, BIG DATA, AI, MACHINE LEARNING AND BLOCK CHAIN

Big data is leading the way in identifying anomalous behaviour within Open banking setups, it is comforting to see retail street banks providing resources to mitigate new fraud risks by implementing controls based on advanced analytics to detect fraud attacks. That detects suspicious transactions and most importantly atypical API calls. This has led to a growth real-time risk analysis being deployed by retail banks as cost effective provision to identify abnormal behaviour in requests originating from third-party providers. Once provisions of GDPR obligations are satisfied with rigorous data protection, block chain technology will be a forefront of KYC diligence, as it will act as an immutable and auditable distributed ledger that will meet EUs 4th and 5th Money Laundering Directive. AI will be able to review client documentation , determine what the legal format is, then elicit the fundamental KYC/ KYB data that will be transpose in support of continued Financial Crime monitoring. Machine learning will have the capability to assess adverse media articles and

transactions then test the materiality of the event or suspicious activity. Thereafter provide an impartial judgment and opine ready for human review. The rise of reg techs digital IDs is negating the costly exercise of navigating through WLF (watch list filters) fussy logic, by having the ability to precisely disposition false positives.

5. CONCLUSION

PSD2 is regulation that in-affect disguises itself as innovation and disruption; innovation will only succeed if the customer journey and user experience is satisfactory.

Big incumbents are innovating to catch up and replicate, but have multiple lines of business, in multiple jurisdictions that need to observer a whole host of regulations. While tackling complex IT architecture that still maintain outdated legacy systems, leading to costly data warehouse projects. On the other hand Fintech banks like Starling and Monzo, who have led this money revolution, have been set up as Greenfield projects. They are more agile and tech driven that can adapt in a nibble way that serves their core demographic needs, ensuring an incredible end user experience at a competitive price point.

Although FinTechs are in an innovative battle to take lead of market share, the industry is collaborating on many fronts such an APIs and hackathons, it is imperative to extend this to compliance risk by standardising best practice that deter criminals from accessing the eco systems front door.

5.1.1 TRUST

Trust is fundamental, throughout the spectrum of generations, trust came be perceived from different pillars. GenTechs and Millennials (born with screens in their hands) are trusting technology companies more, irrespective of social media abuse of data scandal, this only encouraged data subjects to be more privacy savvy and to understand their data rights and controls. Whereas the older generation still rely on bricks and mortar to bank, though there is gradual redundancy as apps become simplified and tech disruption prevails with 24 hour on demand banking.

Trust in the context financial of services has four foundations in which customers expect nothing less;

- Security
- Privacy
- Service
- Integrity

Any comprise of the these foundations will unequivocally lead to a rapid erosion of trust primarily from customers as well as other parties that procure or interface within the Open banking eco system. While many say reputational risk is difficult to quantify, you only have to look at customer attrition rates when things go wrong. Therefore having an effective risk and control framework that meets not just regulatory demand but consumer trust expectation is again critical to survival of a Fintech. Will this embryonic eco system need to keep one step ahead by forging its own controlled environment? That is essential to building and maintaining trust and integrity from its growing but wary customer base and the competent authorities (regulator) who have a vested and imperative role to ensure the financial system as we know it does not go through another period of dramatic loss of consumer confidence, similar to that of the last decade's financial crisis.

When abuse trends emerge, centralised forums like the UKs 'FinTech FinCrime Exchange' communicate abuses typologies to the Open banking ego system affording all participants greater awareness to spot and prevent.

A sound reputation is vital to survive, therefore, using Darwin's Theory; "it's not strongest or most intelligent that survives, it's those that adapt to change"; as and when these new typologies and threats of Open banking abuse emerge.

6. CONTACT

Written by: James Emin (https://www.linkedin.com/in/james-emin-3688985b/)

Contact: **info@lysisfinancial.com**

Date: September 2019