Payment Services Directive (PSD2)

Opening the doors to a secure business

Payment Services Directive
(PSD2)

Introduction

Designed to improve choice for customers, create more competition and stimulate innovation, PSD2 will drive fundamental change in the way we bank. The move to the digital marketplace is no longer an aspiration, but is a necessity for financial institutions to stay relevant or competitive. As part of this evolution, new risks need to be considered in relation to regulatory compliance, privacy, liability and a new attack surface for cyber criminals. These risks are not necessarily greater but different, and need to be treated as such. Success in this new era will be dictated by banks and FinTech's which maximise API integration with third parties in a secure manner. This paper explores some of the fundamental changes that underpin PSD2 and the security model that is changing with it. Although PSD2 is a new regulation, the security challenges are the same as with all Fintech solutions but they manifest in different places across the ecosystem. Questions such as the scope of responsibility and security requirements; "*what are they and where?*" coupled with business risks associated with moving towards PSD2 need to be examined.

What is PSD2 (Payment Services Directive)?

PSD2 is the second "Payment Services Directive", designed by the countries of the EU. It could revolutionise the payments industry, affecting everything from the way we pay online, to what information we see when making a payment. PSD2 provisions bank customers to use third-party providers to manage their finances, such as payment of bills, making P2P transfers, amongst other activities while still maintaining your funds placed in one's own current bank account.

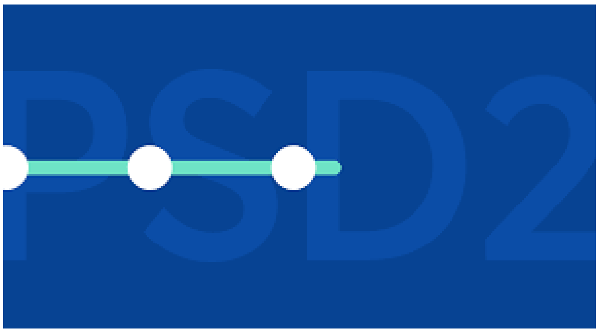
This in effect means banks opening up interfaces to customer data, to third party fintech (Financial technology) providers. Banks will be obligated to provide third-party providers access to their customers' accounts through open APIs (Application Program Interface). This will enable third-parties to build financial services on top of banks' data and infrastructure. The immediate challenge is to develop app-based services that can make the most of this environment. This will inevitably involve banks working with third parties that wish to gain access to customer accounts. But for those banks that provide easy integration for third parties, it is clear they will attract more customers and new revenue models.

This has an obvious upside for banking customers in terms of flexibility and seamless transactions but other aspects of this new model must be considered such as information security, privacy and liability concerns.

How does this enable digital transformation?

Digital transformation is the realignment of an organisation through the use of digital technology to improve the way it performs and serves its clients/users. Customer focus is the core of "digital transformation" - PSD2 radically changes the rules of engagement in the industry, since it gives customers a choice, flexibility and control over the services they use. The transformation will provide banks with an opportunity to "be different" amongst competitors. The ability to operate multiple accounts, activities and services from one application should not be underestimated and will grow the adoption of such services and product offerings; clients will use multiple providers via a single solution. The opportunities for customers are endless, for example viewing all bank statements in one simple view or the notification of cheaper services and products. Convenience is key to PSD2 as it gives clients more flexibility and choice. Early adoption of customers using third party applications is likely to be based on data scraping and analytics of accounts, however credit decisioning through cheaper product offerings will not be far away.

"Seamless payment for services via apps is already a reality and growing. Similar integrations will extend beyond payments into personal finance, investments, invoicing, accounting and much, much more. Open APIs will support seamless, contextual experiences and power us into a new era of client engagement…."



The Web of Security

The EU issued consultation guidelines in 2014 via the European Banking Authority (EBA) regarding the security of Internet payments and the guidelines which should be applied to PSP's (payment services providers)

This has impact on both the banks and also third parties in relation to the security surrounding internet payment activities. The guidelines cover a number of aspects of leading information security practices such as governance, risk assessment, monitoring & reporting, risk control, customer authentication & identification and auditing.

The inclusion of PSP's in relation to PSD2 shall increase the third-party access frequency and proliferation of such services across the banking and financial industry.

The regulation requires that banks operating across Europe expose standard open application programming interfaces (APIs) that will underpin PSD2 and enable their customers to securely share their account data with other banks and third-party providers (TPPs) once they've given their explicit consent.

TPPs may include:

- Account Information Service Providers (AISPs) – Any provider that wishes to aggregate information on one or more payment accounts held with one or more payment service providers who typically present customers with a single dashboard view of accounts. This is useful for upselling/cross-selling financial products among other things
- Payment Initiation Service Providers (PISPs) – Any organisation that initiates a payment where the merchant consumes an API exposed by the bank in order to initiate payments on the basis of a credit transfer

Today, each bank can define their own unique interfaces for TPPs to connect to their services. Standardising on a common set of open APIs will make interoperability a lot easier. It will provide TPPs with a much clearer understanding of what they need to do to connect with banks and provide more innovative online services and applications for customers using the data they would have access to.

Fintech's and PSP's

PSD2 gives third parties (Fintech's) access to data and payments via APIs on behalf of the customer. A financial technology solution/company, also known as a FinTech, is a company that makes use of new technology and innovation with available resources in order to compete in the marketplace of traditional financial institutions and intermediaries in the delivery of financial services.

Many fintech companies supply apps and websites to assist their clients with services such as lending, account balance, payment, financial analysis etc.

Many fintech companies are early stage and agile in relation to pivoting around services offered and development of such services and applications. We have some established players such as PayPal, Amazon, Elavon, Realex but the industry is still in its disruptive phase, emerging, adopting and evolving. The final impact of fintech on the financial services industry is yet to be seen, but likely to introduce radical adoption. The same goes for the impact of fintech and PSD2 on information security, risk and liability and is a moving target to some degree due to the rapid evolution of the industry vertical and regulatory changes.

Industry disruption is generally considered a "good thing" for consumers as it encourages innovation and competition but there are some inherent risks which need to be managed. The risk of fraud, cybercrime, unauthorised access and disclosure of data is still apparent as it ever was in relation to Internet based banking but the actors are different given the introduction of PSP's via PSD2 model.

Here be dragons; The introduction of third parties will bring into question issues like regulatory regime, liability, governance and possibly mind-set or behaviours of the customer; accepting the risk that goes with using a third-party solution to access banking data and services on your behalf.

In saying that, there are some well-established PSP's in the industry which have demonstrated a significant level of trust and have resulted in market share such as PayPal, Amazon, Realex etc. Nearly 50% of all banks plan to provide an open bank offering as there is upside opportunity to service more clients, gain market share, keep pace with innovation and exploit newly introduced financial systems such as crypto-currencies (bitcoin).

> *"The introduction of third parties will bring into question issues like regulatory regime, liability, governance and possibly cultural mindset of the customer…"*

PSD2 Trust Model

The trust model has changed from traditional interfaces between the client and bank to the client giving authorisation to the PSP to act upon its behalf. There are extra "moving parts" in the model and therefore proper governance and information security needs to be adopted in order to protect a client when using intermediary fintech services. From a cyber security standpoint, complexity is always the enemy of security by increasing the "attack surface" (more systems to attack and breach) and more moving parts means just that.

Fintech suppliers need to adopt secure system and solution development and maintenance processes. As per the EBA guidelines they also need run-time monitoring, alerting and management solutions in order to help detect typical threats associated with Internet banking such as Phishing attacks, Banking Malware, hacking attacks and other known threat agents which will also attack both banking infrastructure and fintech solutions as they are deployed.

The usage of a third party will result in a greater distribution of sensitive data across more systems and apps. The traditional boundaries of trust will dissolve and this shall require more due diligence, compliance and a strong security strategy as more and more third parties connect into the eco-system.

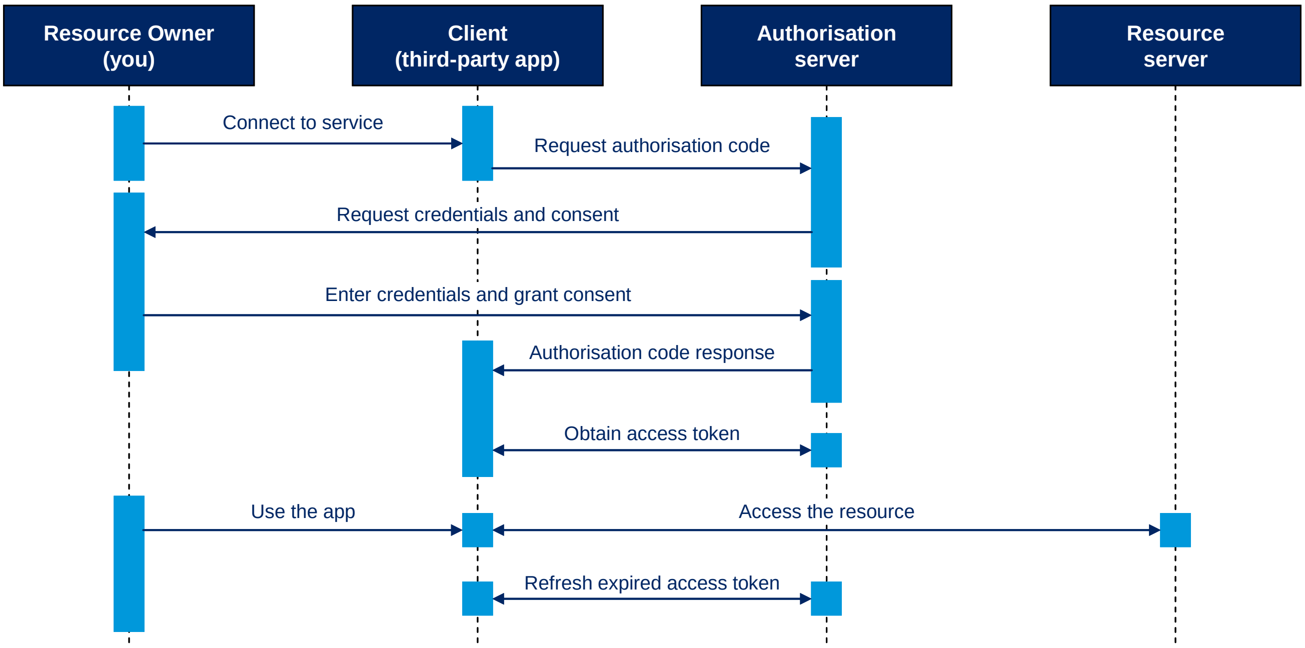
Fundamentally the internet is not a place we trust. Looking back on the adoption of API's within tech companies, the uptake in financial services is likely to be low for some time. By 2020 it is predicted that 20% of consumers will use FinTech's for transactional business.

The Oauth Dance

As we can see there are a lot of moving parts within the flows. A secure Identity and Access Management strategy is a key element of security. The foundation of customer trust will be based on permissions based authorisation, where customers will authorise third parties to populate applications with data through API calls. The foundation of that trust is likely to be built around the Oauth protocol.

OAuth is a protocol that provides to clients a "secure delegated access" to system resources on behalf of the resource owner. It specifies a process for resource owners to authorise third-party access to their server resources without sharing their credentials. Items such as encryption, password complexity are important but unique to OAuth is secret key management. OAuth uses multiple keys to provide access without validation of credentials.

> *"By 2020 it is predicted that 20% of consumers will use FinTech's for transactional business. ..."*


Resource Owner (you)
Client (third-party app)
Authorisation server
Resource server
Connect to service
Request authorisation code
Request credentials and consent
Enter credentials and grant consent
Authorisation code response
Obtain access token
Use the app
Access the resource
Refresh expired access token

As depicted above, credentials are passed to authorisation server and not to a third party. The *Third party does not store user credentials* but stores an authorisation code. The authorisation code needs to time out and invalidate after a defined period. *This reduces the risk of account compromise.*

Minimum security requirements:

It is important to establish minimum security requirements as per EBA guidelines and also to establish if such controls have been tested and operate as expected. In addition, secure application development practices are of paramount importance with consideration to protection against hacking, malware and API abuse.

Third-party authentication:

As per EBA guidelines "Strong customer authentication" is required. Open protocols such as OAuth (https://oauth.net/) and Multi-Factor (2-factor) authentication are required. Re-authentication is also required depending on the activity being invoked such as funds transfer or payment.

API version management:

API's exposed to fintech's need to be managed appropriately. They also need to be assessed such that they cannot be misused. API's are generally released on an iterative basis in order to support more features over time. Version management includes helping ensure technical security controls are implemented on all releases.

Prevention and monitoring:

Vulnerability intelligence and monitoring needs to be continuous such that the banks can't control the client technology being used. Client devices could be infected with malware or breached in some manner. This is issue is not unique to PSD2 but all Internet banking. Monitoring of client activity, anomalies, unexpected behaviour and errors are key to detection of malicious activity and also provide an audit trail of actions undertaken by the fintech application on behalf of the client/user. Data Leakage prevention should be considered also in order to detect such occurrences.

Terms and Conditions of using a third-party solution to access banking data

Users need to be aware of liability when using a third-party solution to access their information on their behalf. The terms should discuss the liability conditions when using third party solutions and any potential risks associated with using technology which is not supplied by the bank to access their data.

Terms and Conditions between a bank and the fintech company

Establishing liability and terms in relation to delivering the service from the bank to the fintech company. Where the delineations between the third parties and the bank in relation to liability and duty of care need to be established and agreed. It is understood that providers who fail to authenticate a transaction appropriately will be held liable for any breaches that occasion a loss.

Security Management Processes

The establishment of formal internal security frameworks by both the bank and the PSP to assess and report on operational matters expressly including security issues. This should include security incident reporting: both to regulators and customers under certain circumstances to be GDPR compliant (see below).

Mandatory security assessment reporting to regulators: on security measures and their effectiveness.

General Data Protection Regulation (GDPR)

Building on the 1995 EU Data Protection Directive, it establishes one set of data protection law across all 28 European states. This results in increased maximum penalties for mishandling data are now 4% of global revenue or 20m Euro, whichever is greater. Responsibility for protecting personal information under GDPR will extend to data processing (Banks, PSP & TPP) as well as data controllers (Banks).

In relation to fintech processing of a client's data the following shall apply and should be considered;

- All data breaches must be reported as soon as possible and, where feasible, no later than 72 hours after discovery of a breach
- Personal data now extends to geographic location, IP address, RFID identifiers, as well as whole new swathes of medical data, including genetic information
- The "right to be forgotten" being enshrined in law, allowing people to request the deletion of data pertaining to them
- The regulation is far reaching across the globe and applies to companies headquartered outside of Europe as long as they have operations in Europe
- It specifies a greater level of rigour around consent to use personal data for appropriate use

- New requirements have been introduced to carry out Privacy Impact Assessments (PIAs) to ensure that personal data is sufficiently protected and privacy of the individual maintained
- Increased role of EBA and ECB: on setting the security protocols, technical standards and policies to be followed in connection with the above obligations

Business Risks to consider

PSD2 has mandated third parties will have to meet certain operational and security requirements before being authorised to obtain data. While this provides a level of protection, it is also clear institutions will need to reassess their own security posture before fully embracing PSD2.. Real risk needs to be assessed based on the appetite of the organisations. For example, the API should be assessed based on the probability and likelihood of system or data compromise by the maturity of the controls that underpin that.

API Governance – APIs are the same as any other technological asset; their continued use should be assessed periodically from a risk management perspective, identified with clear ownership information and subject to security reviews including penetration testing and vulnerability scanning so any weaknesses can be identified and remediated.

Privacy and data flows – With increased interaction between banks and third parties, open banking will increase the complexity of data flows in and out of the enterprise. Data owners should understand the information life cycle and ensure sensitive information is encrypted in transmission and when stored.

Liability – If it goes bad there is more ambiguity, who is to blame? The bank or the third party? Third parties with "access to the account". Account access is controlled by the bank and authorised by the client third Party Service provider error – blame bank? – There is a requirement for Banks to build T&C's which set out the required security standards of third parties, these directive controls cannot be enforced but can offer a level of protection.

Reputational impact – Bank is custodian but authorisation has been given by client to third party to access bank details via app/service. Regardless of the terms in place, a third party compromise or increased fraud as a result of poor management of the API or Third party is likely to cause reputational impact for the Bank rather than third party.

Resilience/Stability – Technical stability, solution lifecycle management and security are considerations.

Disintermediation – Actors shall come between the bank and its customer and change the traditional model, this introduces the risk of client fidelity loss.

Risk Management Recommendations

The risks involved with engaging PSD2 are not greater assuming there is a robust governance structure in place. The risks are not greater… The risks are different.

- Third party actors who supply apps and services via PSP should be verified as secure. Contractually they should undergo continuous security assessment, employ a security management framework and understand the result of non-compliance
- Third Party solution providers should be able to quickly demonstrate the technical controls surrounding their solutions and services where they process client data via the bank
- Bank-level certification/verification of third party apps? "how to police the quality and security of third party solutions?"
- A defined level of security and control assessment should be required in order to prevent third parties introducing an unacceptable level risk to the banking eco system
- The controls used by the third parties should be proportionate to the extent of services offered via PSD2

Conclusion

PSD2 presents significant opportunity for banks to open up product offerings to benefit customers via third party vendors if embraced correctly and managed in a secure manner. The risks associated with PSD2 are similar to any other cybersecurity risks but governance over the protection of user information needs to be considered and broadened to include third party actors. Core security concepts such as secure application development, secure storage, encryption and privacy controls needs to be adhered to and monitored on an ongoing basis.

Adapt or Die – This is the future; PSD2 is a "disruptive" approach to the traditional "client-bank" model but if embraced can enhance a banks product offering, vehicles to market and brand visibility. Clients want flexibility and opportunity to manage their business in a single place. The lack of adoption shall result in lower levels of business, low adoption of new clients and stagnation in the retail banking market. Adoption of PSD2 is key to evolution of the financial industry and should be strongly considered in order to maintain relevance in the financial services industry.

Authors:

Paul Ryan: Head of Information and Cyber Security at Ulster Bank, Ireland. Paul has over 15 years' experience dedicated to Information Security across a wide range of technical disciplines and leadership roles. His focus is on adapting and integrating emerging technical and regulatory changes with security capabilities and leading the Bank through safe change.

Eoin Keary: CEO of edgescan.com and BCC Risk Advisory. Eoin has been involved in shaping the cybersecurity industry for the past 17 years via his involvement in global organisations such as OWASP. Eoin was on the global board of OWASP from 2011-2015 and lead author of many industry standards such as the "OWASP Testing" and "OWASP Code Review" guides and co-author/contributor to books such as "OWASP CISO Guide" and the "Open SAMM Standard"