April 2018

Financial crimes observer

A publication of PwC's Financial Crimes Unit

Open banking: US is next

Open banking is an emerging trend in the financial services industry that is opening the door for third party providers (TPPs) to offer a wide variety of new services – and it is poised to change the traditional retail banking model as we know it. Using open banking, financial institutions can securely provide other financial institutions and TPPs with seamless access to, and communication with, customer data through a standards-based technology called open Application Programming Interfaces (APIs).

A shift towards open banking has been seen across the globe, evidenced by various regulatory initiatives such as the EU's Second Payment Services Directive (PSD2), which requires that banks provide customer data to TPPs through open APIs. In contrast, open banking is newly chartered territory for the US. Although the concept of data sharing with TPPs is not entirely new to the US banking industry or consumers – as there are many US web-based financial management tools that aggregate customer financial data – the method of data sharing has mostly been through a less secure and integrated process called "screen scraping" rather than through open APIs.[1] However, several large banks have recently opened "app stores" that allow TPPs to provide services using open APIs.

Despite its many benefits, open banking will significantly expand the attack perimeter for financial institutions and raise a number of new risks and considerations. Specifically, financial institutions and their TPPs will need to implement effective authentication controls, create clear policies around data governance and data security, and develop mitigation and reporting processes in the event of cyber or fraud incidents.

This **Financial crimes observer** provides (1) background on open APIs currently under development, (2) the regulatory response, and (3) considerations for financial institutions and TPPs going forward.

pwc

What open banking capabilities are being developed?

Financial institutions are in the process of building out the technology infrastructure and security framework to support open APIs. Once efforts have matured, this infrastructure will significantly expand the services available to customers. Examples of such services include:

- *Payments* – While a number of third party payment processors have had success, open APIs would allow customers to skip third parties that take time to clear payments, not only making the process quicker but also increasing transparency and simplicity.
- *Data brokerage* – Third parties could use open APIs to access basic account information in order to make informed decisions based on a customer's financial history, balance information, and other relevant data.
- *Client interface* – Customers could view their own data across a unified platform on a seamless interface and use this platform to interact and transact with financial institutions and TPPs.
- *Identity management* – Open APIs can be used to validate account information and standardize authentication processes among financial institutions and TPPs. This could also provide for more seamless notification of fraud alerts between financial institutions.
- *Account lifecycle management* – TPPs are developing platforms to allow for end-to-end services including account opening, management, and closure. These platforms would allow TPPs to assist the customer manage transactions and make automated decisions

How have regulators responded?

Regulators in the US and abroad have taken a variety of approaches to addressing open banking. The EU has been the most supportive – going so far as to require that banks provide access to TPPs through open APIs – while several Asian countries have provided frameworks and common standards for open banking. US regulators have taken a more hands-off approach by issuing non-binding guidelines and letting the industry lead the way.

Global response

The EU has had the strongest response to open APIs with PSD2 coming into effect earlier this year. PSD2 requires that (a) banks provide access to customer data to third party providers via open APIs, and (b) banks and their TPPs implement related data security controls. Specifically, PSD2 requires that banks and TPPs conduct risk assessments and implement related controls to mitigate identified risks, monitor transactions to identify red flags, and report incidents to national authorities "without undue delay."

Additionally, PSD2 calls for banks and TPPs to apply "strong customer authentication" methods to all but low risk transactions.[2] This includes the use of authentication codes that (a) contain the relevant details of the transaction, and (b) are sent on a separate channel than the one that executes the transaction (i.e., dynamic linking). It also requires that customers confirm at least two of the following three elements (i.e., multi-factor authentication) for all but the lowest risk transactions:

- Something the user knows (e.g., username, password, PIN)
- Something the user possesses (e.g., phone, token)
- Something inherent to the user (e.g., fingerprint, facial recognition)

Banks and TPPs will also have to comply with the EU's General Data Protection Regulation (GDPR), which goes into effect on May 25. The GDPR will require that these firms take a number of steps to protect customer data, including by undertaking privacy risk assessments, having staff dedicated to protecting customer privacy, and allowing customers to request that the firms no longer store their data.[3]

Further, several European industry groups have provided guidance and directives related to open banking. The Open Banking Working Group, a UK based payments industry group, developed the Open Banking Standard Report in 2015 to outline standards for open API development and provide a framework for implementation. In Germany, industry members created The Open Bank Project, which provides an open-code API for banks to access and an app store that brings banks' applications and service offerings to customers. Across the EU, other financial institutions and industry groups are creating similar types of portals for payments service providers, banks, and developers.

In Asia, we are seeing regulatory authorities work to create common standards for open banking. The Monetary Authority of Singapore is working to provide a public API architecture and develop common standards to enable new uses of data by financial institutions. Additionally, Korea is building a public API system for the banking sector to allow FinTech companies to download and leverage technical specifications required for development of products and services.

Where does the US stand?

In the US, several regulatory bodies and industry initiatives have sought to provide guidance and uniformity for open banking, although no regulator has issued prescriptive requirements. For example, the Consumer Financial Protection Bureau (CFPB) released a set of data sharing principles that outline non-binding guidelines for the access and use of consumer data. These broad principles recommend that firms take steps to secure customer data, provide transparency to customers around what data is being collected and how long it will be stored, and offer customers a dispute resolution mechanism. Additionally, the Federal Financial Institutions Examination Council (FFIEC) has released guidance on related topics such as retail payments systems and outsourcing technology services.

Several industry groups have also created frameworks to create common standards for open banking. The Electronic Payments Association (NACHA) has recently created the API Standardization Industry Group, which identified 16 specific APIs for development based on their overall impact to the payments industry. These 16 APIs fall under three categories: (1) fraud and risk reduction, (2) data sharing, and (3) payment access. See **Appendix A** for a full list including the five APIs that have been identified as first priorities. Separately, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has developed an API to support the secure transfer of data and align with PSD2 requirements to help financial institutions use uniform systems when conducting business in the US and EU.

While these efforts and initiatives demonstrate progress, there is currently no pending legislation or regulatory effort in the US similar to PSD2 to create a framework and security standards for open APIs. This may position US based financial institutions at a disadvantage compared to their EU counterparts, who have significantly invested more time and have received more guidance on develop internal capabilities. Additionally, US-based financial institutions with a significant EU presence face an additional set of challenges associated with managing an entirely new set of requirements and business practices as well as potentially disparate approaches for US- and EU-based entities.

Considerations for financial institutions and TPPs

Open banking poses an entirely new set of challenges and considerations for financial institutions and TPPs – particularly for US-based firms, which have not had the same head start as their EU counterparts that have been preparing to comply with PSD2. Regardless, all financial institutions and TPPs should consider the following risks and consider whether they should implement mitigating controls and processes:

Authentication

Open banking significantly expands the perimeter for fraudsters to access sensitive customer data, and as a result, having a robust authentication program is more necessary than ever to verify the identity of customers.[4] Because TPPs will use open APIs for a variety of services, firms should adjust the levels of authentication to the risk of the service provided. For payment processing or executing translations, we recommend that financial institutions and TPPs implement multi-factor authentication, and for higher-risk transactions they should implement additional controls such as out-of-band authentication, which requires user authentication through an additional channel (e.g., telephone call backs, text messages). These firms should also consider using more technological authentication methods such as biometrics and soft tokens (i.e., apps that generate temporary PINs for authentication purposes).

Most EU firms are on their way to implementing these authentication methods as they have been adjusting their programs to comply with PS2. US-based firms are also not far behind as FFIEC guidance as well as the New York Department of Financial Services' cybersecurity requirements call for enhanced authentication, including multi-factor authentication for higher-risk transactions.[5]

Data ownership and governance

Prior to open banking, financial institutions were viewed as the primary owners and guardians of customer data, and regulatory requirements focused on ensuring that they conduct due diligence around gathering customer data and understand the nature and purpose of the customer relationship.[6] However, because open banking allows TPPs to access customer account information, the lines have now blurred around who ultimately owns and is responsible for the security of customer data. As a result, financial institutions should review their contractual arrangements with TPPs and customers to include clearly defined responsibilities for compliance with specific laws and regulations surrounding data ownership.[7]

As many TPPs will be storing sensitive customer data, they should be aware of the risk of cyber and fraud incidents, as seen by recent high-profile data breaches.[8] To prevent or otherwise mitigate against these risks, they should make sure that they encrypt sensitive customer data, including data "at rest" (i.e., stored on hard drives or servers). They should also use behavioral analytics to monitor and detect anomalous activity associated with accessing sensitive data, conduct penetration testing, and train staff to detect and respond to incidents.

Finally, financial institutions should clearly define in their contractual agreements with TPPs policies around the retention and deletion of data. When doing so, they should consider legal requirements to retain data to provide audit trails while balancing the increased risks associated with storing data, the financial burden to store and maintain such data, and GDPR requirements that allow customers to request that firms delete their data. Considering the amount of data that will be collected by TPPs, both financial institutions and TPPs should create data maps to know where all their data is located.

Restricting API access and effective vendor communication

The risk of a TPP being compromised, leaving customer data vulnerable to attack, is a very real concern in open banking. As such, financial institutions need to play a "first responder" type role – identifying when data is compromised and acting to immediately to block all services towards the TPP while the issue is remedied. This requires financial institutions to develop procedures to address such instances rapidly, and develop the necessary technology and controls to restrict API access by vendor. Additionally, the ability to effectively communicate any issues or risks to a TPP that renders an API unavailable remains a key consideration.

Incident reporting

Incident reporting has significantly evolved, where most financial institutions provide nearly instant fraud alerts as well as potential fraudulent transaction alerts that require customers to approve the transaction. However, PSD2 will require that financial institutions perform a risk analysis of financial transactions processed for broader reporting requirements, and as a result they will need to have the ability to generate audit trails and create timely reports. Additionally, various US regulators require financial institutions to report cyber and fraud incidents within 72 hours, and accordingly firms should incorporate associated incidents with TPPs into their reporting programs.[9]

Appendix A: API Standardization Industry Group's 16 APIs Identified for Development (Including 5 APIs Identified for Initial Development in *italics*)

Use Case	API
Fraud and Risk Reduction	• *Account Validation* • *Federal and State Tax Payment Receiver Account Validation for Credit Payments* • *Get Bank Contact Information* • Industry Notification of Account Closure • Payer and Payee Identity Verification • Request Account Token
Data Sharing	• Credit Decisions • Get Account Balance • Get Account History • Marketing Purpose • Single Sign On
Payment Access	• *Interoperability* • *Transaction Status* • Financial Institution Approval/Enrollment of ACH Originators • Human-to-Machine (Internet of Things) • Real-Time Messaging and ACH Network Interoperability for "Credit Push" Payments

Endnotes

1. Unlike open APIs – which allow for seamless data sharing and end-to-end encryption – screen scraping technology requires the customer to provide the TPP with their login credentials for their bank accounts and scans for relevant data.
2. For our advice on developing a robust authentication program, see PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016)
3. For additional information on the GDPR, see PwC's *Operational impacts of the General Data Protection Regulation* (March 2017).
4. For additional information, see the *Financial crimes observer* cited in note 1.
5. For additional information on the New York Department of Financial Services requirements, see PwC's *Financial crimes observer, Cyber: New approach from New York regulator* (January 2017).
6. For example, FinCEN's customer due diligence rule contains a prescriptive regulatory obligation to identify and verify ownership information of legal entity customers. For more information, see PwC's *Financial crimes observer, FinCEN's customer due diligence rule: All systems go?* (April 2018).
7. For additional information on third party risk management, see PwC's *Financial crimes observer, AML outsourcing: You're still on the hook* (August 2016).
8. For additional information as well as our advice on preventing data breaches, see PwC's *Financial crimes observer, Cyber and fraud: How to mitigate and prevent the next data breach* (September 2017).
9. For additional information on US incident reporting requirements, see *A Meeting of the Minds: Emerging Regulation and the Convergence of Cyber and Fraud* (March 2017).

Additional information

For additional information about this **Financial crimes observer** or PwC's Financial Crimes Unit, please contact:

Julien Courbe
Financial Services Advisory Leader
646 471 4771
julien.courbe@pwc.com
@JulienCourbe

Sean Joyce
Financial Crimes Unit Leader
703 918 3528
sean.joyce@pwc.com
@RealSeanJoyce

Jeff Lavine
Financial Crimes Unit Chief Operating Officer
703 918 1379
jeff.lavine@us.pwc.com

Genevieve Gimbert
Fraud Management Leader
646 471 5145
genevieve.d.gimbert@pwc.com
@GenGimbert

Vikas Agarwal
Financial Crimes Technology Leader
646 471 7958
vikas.k.agarwal@pwc.com

Roberto Rodriguez
Director of Regulatory Strategy
646 471 2604
roberto.j.rodriguez@pwc.com

Contributing authors: David Fapohunda, Abhishek Gupta, and Erika Rendeiro.

Follow us on Twitter @PwC_US_FinSrvcs

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 223,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us