Open banking

Are the rewards worth the risks?

Risk Universe
by RiskBusiness

An emerging technology is starting to generate buzz and it's Open Banking. Certainly, Open Banking promises much – such as reduced transaction costs, faster transactions and engagement with whole new initiatives such as the pension dashboard. However, there are significant risk management challenges that Open Banking creates, too. This article looks at Open Banking, including its potential and its risks and ultimately concludes that an innovative new technology such as Open Banking may need a fresh, more collaborative approach to risk management, too.

WHAT IS OPEN BANKING?

Open Banking is a global project, taking different forms in individual jurisdictions. The Open Banking project in the UK was created to make it easier for customer data to flow between financial services firms and third parties via APIs. It grew out of the EU's Payment Services Directive 2 in 2015, as well as work by the UK's Competition and Markets Authority (CMA), such as the investigation it did between 2014 and 2016 into the retail banking markets. The CMA's work led directly to an order requiring the country's nine largest banks to enable consumers and businesses to access their personal and SME accounts through third party providers. The CMA also required the nine UK banks to develop an Open Banking Implementation Entity (OBIE) that would set common standards for third party access via APIs.

After a slow initial start, Open Banking has seen significant growth over the past 18 months. Some recent Open Banking statistics include:

- Some 4.5 million regular users of open banking of which 3.9 million are consumers and 600,000 small businesses.
- A 60% increase in new customers (up from 2.8 million in December 2020). One million new regular or active users are added every six months.

- At the end of 2021, cumulatively over 26.6 million open banking payments had been made. This is an increase of more than 500% in 12 months.

Key trends that are encouraging the growth of Open Banking include the rapid decline in the use of cash for payments, the growth in ecommerce as a result of the Covid-19 pandemic and continuing regulatory reforms, aimed at reducing the costs to merchants associated with card payments.

Looking forward, one study suggests that 60% of the UK population will be using open banking by September 2023. Another study predicts a £7.2 billion revenue opportunity in 2022 and that 71% of SMEs will adopt it by 2022. It's clear that the technology is gaining momentum and that it will likely permanently alter the payments landscape before the decade is out. It is also clear that it will create a host of new risks for financial services firms.

WHAT DOES OPEN BANKING ENABLE?

Today, the UK Open Banking ecosystem extends far beyond the original nine banks that started it. There are more than 330 regulated firms made up of over 230 third party providers of services and more than 90 payment account service providers who together account for over 95% of current accounts engaged with the Open Banking initiative. Applications using Open Banking's account information data-sharing functionality include:

- services to establish the affordability and eligibility of a loan in mortgage applications comparison.
- services which identify the best bank accounts for small businesses.
- services which alert customers to potential cost savings, for example, that their mortgage has switched from a fixed to a floating rate.

Recently, NatWest was the first UK bank to conduct a live transaction using Open Banking-initiated Variable Recurring Payments (VRPs). VRPs enable customers to connect authorised payments providers to their bank account so that the payment providers can make payments on the customer's behalf within agreed parameters. Potential use cases for VRPs include:

- automated payments for electricity bills, up to a £100 per month;
- connecting a bank account to a social network app for in-app authentication of payments;
- setting a limit of six months of payments for a new subscription;
- automated payments of ride-hailing fees, up to £45;
- one-time payment set-up for one-click payments offered by an online marketplace;
- using a third-party smart saving app to move money between bank accounts to a savings account on a flexible / variable basis;
- using a third-party service that monitors bank accounts and maintains a threshold balance, or helps avoid overdraft fees by moving funds as and when required between accounts;
- obtaining short term credit to avoid overdraft, then automating repayments

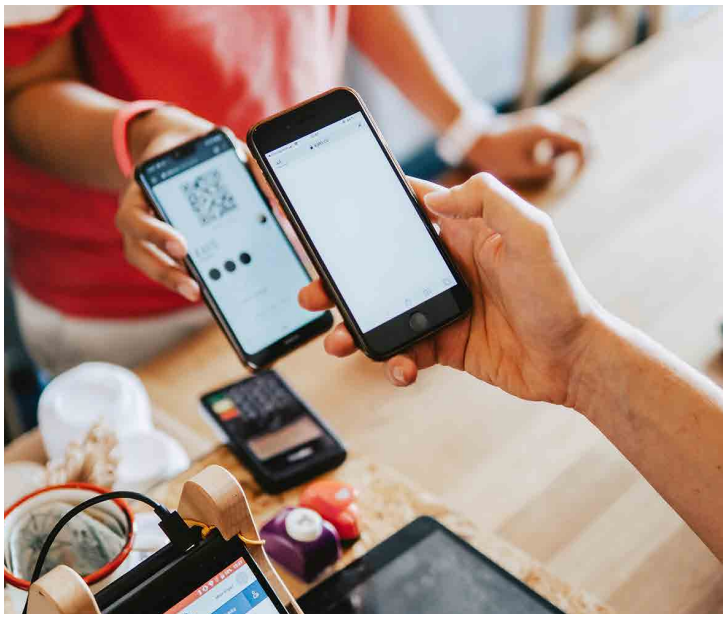
The rapid decline in the use of cash is encouraging the growth of Open Banking

FinTechs may not have the risk and control frameworks in place that most financial firms have

to credit to minimise overdraft fees and borrowing costs.

All of this is very exciting indeed for consumers, merchants, FinTechs and even the banks themselves. While the substantial profits gained from card fees will decline, ultimately implementing Open Banking should enable financial firms to switch off aging technology infrastructure and develop new products and services.

However, the risks associated with Open Banking are also becoming more evident too. While some risks may be worked out as the technology evolves and technological solutions are adapted, other risks may be an inherent part of the Open Banking model. Some risks may accelerate as Open Banking usage increases, while other risks decrease as the ecosystem becomes more mature. Below are five of the risks that could be potential issues for financial firms engaged with Open Banking.



1 THIRD PARTY RISKS

There are risks associated with the third parties within the Open Banking system, including potential process risks, technology risks and data risks. For example, many of the FinTechs involved in developing Open Banking solutions are start-ups that may not come under the aegis of a financial services regulator. As a result, they may not operate to the same compliance requirements and industry standards as regulated financial firms.

Also, there are process risks such as the misuse of customer data, broken or the absence of appropriate process controls, or poor data governance. FinTechs may not have the risk and control frameworks in place that most financial firms have today.

Technology risks can include possible information security or cyber security breaches because of lower or poorly maintained security protocols. The data risks include all of the traditional data risks associated with third parties – but magnified because of the speed at which transactions take place between the customer, the third party and the financial firm.

2 AML RISKS

There are also significant concerns that AML, counter-terrorist funding and KYC processes that firms may currently have are insufficient to meet regulatory obligations within an Open Banking context. For example, financial firms need to ensure that the third party FinTechs they are working with meet the same financial

crime regulatory obligations that are applicable to them. Extending this, some FinTechs may be unfamiliar with the robust regulatory standards that banks have to meet when onboarding customers. However, many financial firms do not have robust enough third party risk management programmes in place to ascertain the level of third party compliance.

There are other financial crime risks too. For example, third parties can limit a financial firm's visibility into how funds flow in and out of its systems and through the wider Open Banking ecosystem, making it more challenging to identify suspicious activity. Indeed, overall, the traditional banks will have less of an overview of the transactions their customers engage in, making it harder for them to identify suspicious activity. There is no precedent for how such a network of transactions should be monitored for money laundering or terrorist financing.

3 FRAUD RISKS

There are also concerns that Open Banking will provide fraudsters with a new channel through which to commit their crimes, leading to an increase in fraud within the UK.

While Open Banking doesn't create new fraud risks, it does provide the possibility that fraudsters will gain access to customers personal data through FinTech third parties and use that data to obtain money by initiating payments and pulling money from the customer account at their bank. Two key fraud scenarios are:

- Account Takeover – Criminals use compromised credentials to access an existing customer account and initiate unauthorised payments; and
- Payment Scams – Conning or using social engineering to get the customer to authorise payments for illegitimate purposes.

At the moment, no data on fraud committed using Open Banking platforms is available. This may be because the use of Open Banking is still limited and so not worthy of criminal attention. However, as Open Banking continues to develop, it seems likely that it will attract the interest of more fraudsters. To address this, Open Banking has several tools on its website and a committee focusing on this issue – but is this enough?

At the moment, no data on fraud committed using Open Banking platforms is available

4 OPERATIONAL RESILIENCE RISKS

As the Open Banking initiatives gathers momentum, it's clear that many of the business processes supported by Open Banking technology and third parties will become important business services and therefore, subject to operational resilience requirements. The newness of the Open Banking technology and the complexity of the network as it grows means that it's likely that there will be fresh operational resilience challenges, which may be difficult for firms to engage with on an individual basis. For example, if a cyberattack takes down a FinTech third party that delivers an important business service to multiple financial firms, how should the third party respond? How should the financial firms respond? Should resilience plans be coordinated across all stakeholders or are firms responsible for figuring this out on their own?

It would seem sensible that operational resilience should be embedded in an early stage of this initiative

It may be that the Open Banking initiative may need to engage directly with operational resilience issues more aggressively – at the moment a search of the website for the term returns zero results. It would seem sensible that operational resilience should be embedded in an early stage of this initiative.

5 ORGANISATIONAL AND CULTURAL RISKS

The Open Banking organisation itself is the subject of an ongoing scandal. A 2021 review by Alison White, an independent chair, found that many of the issues flagged by whistle blowers – such as conflicts of interest and a toxic culture – were true. Furthermore, there was a lack of adequate corporate governance within the organisation, which enabled these issues to spiral out of control. As a result, Imran Gulamhuseinwala, the implementation trustee of the Open Banking Implementation Entity (OBIE), resigned at the end of September 2021.

In response to Alison White's review, in November 2021, the CMA appointed Kirstin Baker, an independent non-executive director of the CMA, to lead a review to identify the lessons for the CMA in its approach to designing, implementing and monitoring remedies in its market investigations. In March 2022, the CMA published its response, outlining the changes that the Open Banking organisation would be making.

The Alison White report does not make for easy reading – in places it is the sort of toe-curling thing that no chief compliance officer or chief risk officer ever wants to read about their own organisation. It remains to be seen over time how well the issues outlined in the Alison White report are addressed. In the meantime, financial services firms need to take these organisational and cultural risks into account when engaging with the OBIE and ensure that these issues do not "bleed through" to their own organisations.

CONCLUSION

While Open Banking certainly holds much potential, financial services firms need to ensure that their approach to managing third party risk is up to the level of robustness required to engage with this new technology and the network ecosystem that comes with it. Moreover, there are several risk types that firms regularly engage with that could be exacerbated by the nature of the network ecosystem, such as AML risk, fraud risk and operational resilience risk. Truly managing

these risks will require the efforts of individual firms, of course. However, it also seems obvious that the network ecosystem nature of Open Banking demands a network ecosystem approach to managing these risks, which is probably best coordinated by the OBIE itself. The bad news here is that the OBIE has itself been the focus of a substantial scandal recently, which has seen its CEO resign and its culture branded as "toxic" – which leads one to consider that the organization's compliance and risk cultures may not be all that they should be. The banks engaged with Open Banking may need to take action. Furthermore, three major banks, including most recently HSBC in April 2022 have been subjected to regulatory warnings for failing to fully comply with the Open Banking requirements. So, financial firms should seek to actively manage the risks associated with Open Banking – while not being blind to the opportunities this new technology creates.

RESOURCES

Open Banking Expo – Moneyhub and Bud to take part in initial UK pensions dashboard testing

World Economic Forum – What's next for Open Banking?

EU -- Payment services (PSD 2) – Directive (EU) 2015/2366

CMA – Retail banking markets investigation

CMA – Retail Banking Market Investigation Order 2017

The Open Banking website

Open Banking press release: UK open banking marks fourth year milestone with over 4 million users

Truelayer – The Future of Ecommerce Payments

PWC – The future of banking is open

CMA – Update on Open Banking

NatWest initiates first live Variable Recurring Payment transaction

Open Banking – Variable Recurring Payments. What are they and how can they help SMEs?

Bird & Bird – Developments in Open Banking: Variable Recurring Payments and Sweeping

Risk Universe
by RiskBusiness

Teradata – Look out for the risks in Open Banking

Fico – 8 Risks Open Banking Poses to Financial Crime Compliance

Finextra – Will Open Banking lead to the Next Wave of the UK's Fraud Epidemic?

Open Banking – Built on Security

Investigation of Open Banking Limited – Independent report by Alison White

Financial Times – UK open banking boss resigns following report into 'bullying and intimidation'

Open Banking press release – The Open Banking Implementation Entity (OBIE) welcomes the Competition and Markets Authority's (CMA) recommendations on the future arrangements for open banking and the Joint Regulatory Statement

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

Contacts

Mike Finlay, Chief Executive:
mike.finlay@riskbusiness.com

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

Risk Universe
by RiskBusiness

www.riskbusiness.com