Deloitte.

Open banking

What does it mean for financial crime?

June 2018

The evolution of an open banking model, where customers rather than each financial institution control and share their data, will potentially have a profound effect on financial crime risk management.

Even though financial crime issues are a significant factor in the design, implementation and operation of open banking, the recent Farrell Report provided only limited comment on the financial crime implications of open banking.[1]

In their submissions to the Farrell review leading financial institutions highlighted their concerns that open banking may result in a significant increase in financial crime.[2] This paper explores the potential impact of financial crime issues resulting from open banking on risk, regulatory and reputational outcomes.

Financial crime regulators will face new challenges in standard setting, monitoring and supervising the potential risks that could emerge as a result of the disaggregation of traditional banking value chains and the corresponding need for financial institutions to manage more agents and sub-agents.[3]

These risks will vary across the following four non-mutually exclusive operating models which are likely to emerge from open banking[4]:

- **Full-service provider:** continue with a full-service offering, delivering proprietary products via a proprietary distribution network
- **Utility:** provide infrastructure and non-customer-facing services, relinquishing ownership of products and distribution
- **Supplier:** offer proprietary products but relinquish distribution to third-party interfaces
- **Interface:** concentrate on distribution of third party products and services by creating a marketplace interface.

As the market for financial services and products diversifies and fragments, and the operating models of institutions change to meet the challenge, the way financial crime risk is managed will be critical.

While inevitably open banking will introduce a number of unknown impacts, there are three areas where the risk will be highest.

Notes

[1] The Australian Government, the Treasury, Open Banking customers' choice convenience confidence, Scott Farrell, December 2017. See also: https://static. treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[2] See also: https://treasury.gov.au/consultation/review-into-open-banking-in-australia/

[3] The Australian Government, AUSTRAC Insights from Compliance Assessments: Good business practices and areas for improvement, December 2016, p8. See also http://austrac.gov.au/businesses/obligations-and-compliance/insights-compliance-assessments

[4] Deloitte, Open Banking, How to flourish in an uncertain future, June 2017. See also: https:// www2.deloitte.com/uk/en/pages/financial-services/articles/future-banking-open-bankingpsd2-flourish-in-uncertainty.html.

Disaggregation and the growth of new players

Both the disaggregation of traditional banking value chains (e.g. through marketplace platforms) and the growth of new players increase the complexity of the financial services market. They also increase and accelerate the risks of financial crime. As customers use a broader range of service providers for their financial services requirements, the proportion of transactions processed by any one organisation reduces, different types of transactions may be processed by a range of niche players, and the complexity of end-to-end processing chains increases.[5]

As a result, individual organisations may have a more limited view of the overall activities of their customers, making it harder for any one organisation to monitor and identify unusual or suspicious behaviours. As the market continues to grow, and each organisation's share of transactional volumes decreases, traditional methods of transaction monitoring and other established financial crime controls will become less effective.

Data sharing: Currently data sharing protocols have been designed to cover a small number of institutions. Although there are some informal and emerging protocols for sharing intelligence and information of customers suspected of breaching local and international laws between financial institutions, they are not yet highly developed. Enhancing data sharing protocols will be important as the range of service providers broadens.

The Fintel Alliance, a public/private initiative led by AUSTRAC, may offer a bold new way of identifying and sharing financial crime intelligence across marketplace platforms. Subject to any legal and regulatory challenges, including the presence of unregulated service providers in the marketplace platform, the collation and provision back into financial service organisations of intelligence across value chains may well be the most effective means of identifying and preventing financial crime in the future.

Regulatory status: Under current definitions of financial institutions it will be challenging to capture all participants in the marketplace platform.[6] Where both regulated and unregulated entities operate on a marketplace platform they can bring different cultural, commercial and operational models for financial crime risk management.

This creates potential conflicts around governance, infrastructure standards and investment with respect to shared financial crime obligations. Financial institutions which are already regulated by AUSTRAC may feel they are expected to bear the burden (and expense) of financial crime monitoring, to the benefit of new market entrants. The regulatory position on this issue will be critical, including further guidance on outsourcing services as well as legal and regulatory obligations across the marketplace platform.

Monitoring and standard setting: As the market for financial services diversifies, regulators will also face challenges in financial crime monitoring and standard setting. Regulators will need to monitor a growing number of smaller players that may be using new, and possibly anonymous, transaction technologies and diverse sources of customer verification data. Even the regulator's role could be compromised if there are inconsistencies or omissions in regulatory guidance or expectations reported across market place platforms.

In recent regulatory forums it has been suggested that fintechs may play a role in providing a central hub or clearing house.[7] Unless the marketplace fosters the development of a 'hub' or 'clearing house' for information and transactions regulators will remain accountable for monitoring the entire market for financial crime risk.

The Farrell report primarily focusses on open banking within Australia yet banking is a global industry. Financial crime control failures have resulted in numerous regulatory prosecutions and fines by regulators in the last decade. Open banking protocols need to consider the extent and potential impact of changes to the Australian banking system on both global participants, and on Australian banking institutions in their offshore businesses.

In respect of financial crime risk management, this may include:

- Nature and extent of regulation across marketplace platforms
- Interrelationship with 'open banking regimes' in other jurisdictions
- Consideration of the use of 'equivalent regimes' and passporting of overseas participants.

Notes

[5] ibid p7

[6] Section 6 Designated Services of the AML/CTF Act (2006) AML/CTF Act defines Financial Services for types of entities (such as Authorised Deposit-taking Institutions) and for categories of activity (such as account opening, transactions, accepting deposits and lending). See also http://www.austrac.gov.au/sites/default/files/documents/amlctf_act_sec6_designated_services.pdf

[7] Tripartite seminars involving the RegTech Association of Australia, AUSTRAC and Deloitte, October 2017.

Customer onboarding

Onboarding is the gateway to the financial system, and the 'front door' for financial crime, but open banking will push institutions to innovate faster and become more responsive to customers. This changing relationship with customers means that customer onboarding standards, processes and controls will inevitably need to adapt and change. Identifying and managing the increased risk will be critical. Both traditional financial institutions, as well as new fintechs and techfins, want to simplify the customer onboarding process using digital channels to accept new customers.

Processes: Simplifying and standardising the onboarding process can start with better utilisation of existing customer information to prevent customers having to fill out yet another form (digital or analog). Biometrics, such as fingerprints, facial prints, voice patterns and retina scans are increasingly available. It might also be possible, subject to regulatory approval, to use non-traditional data sources, such as social media sites, screen-scraping or selfies, to provide new options for electronic identification (eID) verification.

Identity theft: Given that almost 10% of Australians are the victim of identity theft[8] increasing the number and nature of data sources available to identify and verify customers could increase the risk of identity theft or the creation of fraudulent profiles. These problems may be exacerbated if the identity of international customers is verified using global data sources that are not subject to rigorous testing for reliability and accuracy.

As the number of financial service providers increases, some smaller entities may choose to simply rely on the eID verification processes of more established financial institutions. We are beginning to see more utilities providing centralised eID verification services for Know-Your-Customer (KYC) obligations or centralised anti-money laundering/counter terrorism-financing (AML/CTF) transaction monitoring services.

Controls: The Farrell report noted that eID services would be more efficient if undertaken centrally and provided as a commodity to all parties, while noting its legal application would require a change in the existing AML/CTF legislation.[9]

To stay compliant, reporting entities that choose to rely on other parties' eID verification processes, or that use non-traditional data sources, will need to ensure that current requirements are well understood, accurately implemented, and meet minimum regulatory KYC requirements, including an assessment of the reliability and independence of data sources used to perform the eID verification (whether directly or by third parties).

To mitigate the risks, some financial institutions might seek to assure the effectiveness of KYC standards for all parties in their value chain by making it a contractual obligation to not only sign-up to agreed KYC standards but also regularly attest to the effectiveness of the KYC processes and have them subject to independent audit.

But centralisation also introduces systemic risk if all financial institutions rely on the same KYC intelligence, particularly where there are weaknesses in the onboarding controls of the entity providing the information. It also raises the risk that identity theft could, without appropriate safeguards, have significant and systemic adverse consequences across the marketplace.

Standards: There are risks if KYC standards are over commoditised. While this approach will work for standard identification requirements (such as name and date of birth), it would weaken the environment if unique KYC risk attributes (such as the source of funds and the nature and purpose of an account) were commoditised and not periodically refreshed.

KYC is just one component of a modern day financial crime prevention program. There are numerous other obligations including monitoring of transactions, enhanced due diligence and regulatory reporting. Future regulatory compliance strategies will need to determine the responses across marketplace platforms where collective accountability means organisations in a marketplace platform are only as strong as the 'weakest link'.

Notes

[8] Australian Institute of Criminology, Identity fraud and theft in Australia, Crime Facts Info No 164, Canberra, published Feb 2008, last modified Nov 2017. See also: https://aic.gov.au/publications/cfi/cfi164.

[9] The Treasury (2017), op. cit, pages 34-39.

Assessing the risks of new products and services

As new products and services are developed, it will be important that the financial crime risks and threats for these products and services are identified, understood and controlled.

Financial crime regulatory requirements need to be considered alongside customer experience and conduct considerations whenever a new product or service is being developed. Increasingly, financial crime regulations require an assessment of all financial crime risks before a product or service is offered to customers. If this is not done well, or fails as a result of poor process and control design and execution, there is a risk that the product or service developed may enhance customer experience, but expose the organisation, and so indirectly the customer, to financial crime risk and associated penalties.

Assessing the financial crime risk: All participants in a marketplace platform will need to undertake their own financial crime risk assessment. Under current regulatory requirements financial institutions need to assess the aggregated risk of their products, services, customers, channels (including agents) and jurisdictions being vulnerable to exploitation for illegal activity (either directly, or to launder illegal proceeds). This assessment should direct the development of a financial crime risk appetite statement that is endorsed by the Board and Executive, and guide the organisation on its financial crime parameters or tolerance as it rolls out its future commercial strategy.

It is likely that other service providers in a marketplace platform will need to undertake their own financial crime risk assessments, either under law as a result of regulatory status (i.e. as a reporting entity), or through contractual agreement with a regulated party.

As financial crime compliance is increasingly undertaken on a risk based approach, it will be helpful to align risk profiles across marketplace platforms to design and deliver sustainable and regulatory defensible processes.

Increased automation risk across the marketplace platform: Where risk failures occur as a result of an algorithmic or automated process, there is a much higher risk of both repeated and far reaching non-compliance. Erroneous automated processes can result in significant operational, reputational and financial consequences.

Where new products or services include an offshore element (e.g. payments, crowdfunding or peer-to-peer lending) it may be that standard KYC or AML/CTF compliance processes are less effective. Designing and implementing enhanced customer due diligence standards and monitoring customer activity, including payments, across the marketplace platform may be inhibited by product and system limitations, or complex outsourced risk management, including transaction monitoring. If something goes wrong, there is every likelihood that the regulatory risks impacting the Australian financial system from offshore regulators will continue with significant financial penalties and orders for costly remedial activity for non-compliant activities.[10]

The introduction of open data also creates opportunities for financial institutions to distribute non-banking services. While this may require licensing and/or regulatory approval, the move away from only core offerings to a broader ecosystem could introduce a greater level of financial crime risk.

Notes

[10] The principal offshore regulators are the US Office of Foreign Assets Control (OFAC), the UK's Financial Conduct Authority (FCA), Singapore's Monetary Authority of Singapore (MAS), and the Hong Kong Monetary Authority (HKMA)

Consents and permission

Currently many new entrants, particularly online businesses, ask customers to share banking usernames and passwords. This exposes those customers to possible online fraud, as well as the danger of breaching the terms and conditions of their banking relationship. This in turn compromises their ability to seek restitution for any subsequent losses.

Some of the hurdles: The reality is that open banking may result in overt attempts by criminals to pose as representatives of new service providers in order to obtain confidential access information. As always, controlled data management is an imperative in minimising financial crime risk.

As customers authorise their financial institutions to share their information, the institution will need to have robust consent and permission systems, processes and controls to be able to validate those requests (particularly online) and avoid inadvertently sharing information with the wrong counter-party.

In addition, as part of their broader fraud and AML/CTF obligations, financial institutions will also want to ensure that the third party requesting information is legitimate and accredited.

Certain customer information gathered under financial crime laws cannot legally be shared with customers or be used for broader commercial purposes. In an open banking environment, organisations, particularly those in a marketplace platform, will need to carefully quarantine such financial crime related customer data.

Data: Customer data management in open banking is likely to involve a series of trade-offs. However, regulatory and risk considerations for financial crime data management may act as a boundary constraint on these options.

Third parties: One challenge will be managing multiple third party requests for access to customer data, particularly where the request or subsequent consent differs in any material detail. Where this occurs extra controls across the ecosystem will be necessary to manage this arbitraged information and prevent any inadvertent unauthorised release of information. To avoid this, we expect the industry to provide granular guidance and/or templates to facilitate consistent release under consent.

More protocols: While protocols for the consent and release of information create one challenge, protocols around revoking consent could create another. This can create challenges in lead times as well as a knock on effect with one provider potentially creating issues further down the ecosystem. Industry protocols could go a long way to minimising these impacts and providing greater certainty and transparency to all stakeholders.

Education: Finally, consumer education will be very important in the new world of open banking if customers are to avoid being impacted by financial crime. Regulators, financial services providers, technology providers, industry bodies and consumer groups will all need to closely monitor developments and inform the broader public of risks and preventative strategies.

Key questions organisations should ask

As we consider future financial crime risks in an open banking environment, organisations should consider the following questions about their financial crime exposures and processes:

1. Have we undertaken sufficient due diligence to understand the impacts of open banking on our financial crime strategy and program?
2. What involvement and signoff will financial crime officers have in process and control design across marketplace platforms?
3. How will we ensure our financial crime solutions across the marketplace platform are compatible with the market – protecting our reputation but without creating commercial disadvantage?
4. How will we manage the lead times to extract and integrate customer information from old and complex legacy systems?
5. Have we documented the end-to-end processes of the marketplace platform to understand upstream/downstream operational and regulatory impacts?
6. What operational and communication protocols will we want to insist on to identify and react to a financial crime incident?
7. To avoid exposure to the 'weakest link', especially at hand off points in a process or value chain, what needs to be in our service level agreements with providers in the marketplace platform?
8. What level of access and control assurance will we need to manage financial crime risks across a marketplace platform?
9. Where a service provider in a marketplace platform receives regulatory censure, what should be communicated to other participants of the chain, and how?
10. What legal and regulatory changes are likely to enable regulators to support ongoing financial crime risk management in a world of open banking?
11. How will we align processes and controls in a marketplace platform, where views on financial crime risk differ?

Last word

As Dylan said "The times they are a changin'", and in open banking there will be significant changes for financial institutions, service providers, consumers and regulators. In that shadow world of the criminal, as they wait in the wings and watch events unfold, whether as organised gangs or opportunists, any weaknesses in operating systems and controls will be probed for exploitation at every opportunity.

The combination of significant organisational and environmental change, together with significant numbers of new players to the industry, creates a perfect storm for new financial crime vulnerabilities. Identity theft alone has the potential to cause greater systemic risk and loss than we have yet experienced. This means that the nature and positioning of regulatory accountability and oversight will be a significant determinate of financial crime risk in the new regime.

Financial institutions and regulators will require critical and innovative thinking to identify and mitigate the burgeoning financial crime risks in this brave new world of open banking.

The Russian proverb, 'trust but verify', will become an important mantra for all financial institutions across the marketplace platform.

Contacts

Chris Cass
Principal Financial Crime
+61 418 509 360
ccass@deloitte.com.au

Lisa Dobbin
Lead Partner Financial Crime
+61 435 294 118
ldobbin@deloitte.com.au

Series editor

Paul Wiebusch
Partner, Financial Services
+61 3 9671 7080
pwiebusch@deloitte.com.au

MCBD_Syd_06/18_055432