Deloitte.

Open banking, open risk?

Managing financial crime in a disrupted world

Contents

Preface

The financial services industry is changing faster than at any time in the last half century. New technologies, new entrants to the industry, new regulations and changing consumer preferences are combining to disrupt and fragment what was until recently an industry dominated by the major banks.

Traditional retail banks face stiff competition from new market entrants, including challenger banks and technology-based financial service providers ('FinTechs'), that are often more agile and less constrained by costly legacy systems than their conventional competitors. At the same time, regulatory changes are creating a new "Open Banking" environment, that has the potential to diminish ownership of the customer relationship by larger retail banks.

Our analysis and research, combined with the views of our clients, indicate that these changes will have a profound effect on financial crime risk management at both an institutional and market-wide level. New financial crime risks will need to be mitigated to combat money laundering, terrorist financing and fraud. Furthermore, we consider that existing approaches to financial crime risk management may become less effective at identifying and mitigating these risks, and that the roles and responsibilities of those involved in financial crime risk management will need to rebalance to reflect the shifts in the industry.

We see a range of possible ways in which this might work, from greater reliance on banks to manage risk on behalf of other financial services providers, through to market-owned utilities providing financial crime risk management services to all players.

Regardless of the model, it is clear that banks and FinTechs will need to interact and collaborate more, with the support and engagement of relevant regulatory bodies. This becomes even more vital as the industry shifts to an open banking environment, where shared customer data is the norm.

The challenges facing the industry are significant and the outcomes are far from certain, but it is our view that regulatory and market change has now reached an inflection point where financial service providers need to re-examine the fundamentals of their approach to financial crime risk management and reporting.

This is a continuing discussion, and we welcome contributions from all parts of the financial services industry. The days of stand-alone solutions to problems of risk and compliance are gone: a collaborative debate is what we need now.

"Financial service providers need to re-examine the fundamentals of their approach to financial crime risk management and reporting."

New banking models emerge

The impact of regulatory change on incumbent banks across the EU as well as in the UK has been explored in Deloitte's recent paper on *Open banking: How to flourish in an uncertain future.* This report explores the impact of the EU's recently revised Payment Services Directive, known as PSD2, and the decision of the UK's Competition and Markets Authority (CMA) to mandate UK banks to adopt the Open Banking Standard. Our analysis together with survey results from YouGov on the personal and SME banking sectors suggest that the opening up of customer data to multiple financial service providers through a single banking interface will reshape the market, and potentially lead to the decoupling of products from distribution.

In this increasingly diverse and fluid marketplace, we suggest that established banks can choose from four non-mutually exclusive operating models.

The full service provider continues to deliver proprietary products via a proprietary distribution network.

However, this option is unlikely to prove the optimal model in a future of increased competition from established and challenger market participants. We expect that most banks will opt to combine one or more new models.

The **utility** will relinquish ownership of products and distribution, and concentrate on operating as a provider of infrastructure and non-customer-facing services.

The **supplier** will offer proprietary products but relinquish distribution to third-party interfaces.

The **interface** will concentrate on distribution of third party products and services.

Market and regulatory changes imply a shift from a product-centric to a customer-centric model. The shift opens the opportunity for banks to begin servicing 'adjacent' customer needs. An example of this could be building an ecosystem of different providers that allows customers to purchase an end-to-end package of services within complex transactions, such as buying or selling a house or business.

A continued focus on financial crime

Managing the risks associated with financial crime is an increasingly acute and complex challenge. Regulatory pressure has been growing, with bodies such as the Financial Action Task Force (the multilateral organisation that sets international standards on money laundering and terrorist financing) becoming more proactive in shaping the regulatory environment. In the UK, regulations are intensifying with initiatives such as the Financial Conduct Authority (FCA) Senior Managers Regime. This requires bank executives to take personal accountability for managing financial crime risks, and the FCA has recently proposed that the regime be extended to all regulated financial companies.

As a result, banks are devoting greater resources to managing their financial crime risks. Increased regulatory scrutiny combined with a number of high profile enforcement actions have prompted banks to undertake large scale remedial programmes to establish a more robust financial crime control environment. They have also undertaken comprehensive risk assessments including the screening of customers to identify high risk factors, and applying enhanced monitoring of transactions for suspicious activities. Moreover, stronger governance is encouraging executives to oversee and manage financial crime risks better.

"Banks are devoting greater resources to managing their financial crime risks."

Yet, despite the enhancement of risk management, the underlying mechanisms of risk mitigation have remained the same. Customers are still required to provide information at 'on-boarding' (the point at which financial service providers take on new customers), while transaction monitoring continues to score the flows of transactions in and out of the bank against a number of pre-described scenarios. These activities may be more streamlined but they are not new. Due diligence is limited by the point-in-time nature of customer information and by the scope of an organisation's customer profiling.

As the market for financial services diversifies and fragments, regulators face new problems in financial crime monitoring and standard-setting. Regulators are likely to find it increasingly difficult 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.

And the question remains: in the evolving world of financial services, does the way that banks, regulators, and more recently FinTechs, manage financial crime risks remain appropriate? We believe now is the time to re-examine the overall approach, to review what risks are emerging and what responses are necessary.

"Regulators are likely to find it increasingly difficult to monitor a growing number of smaller players that may be using new and possibly anonymous transaction technologies."

Emerging risks I
The changing customer dynamic

Market changes mean that customer on-boarding controls are increasingly unfit for purpose.

The typical customer no longer expects to buy financial services from a single provider. Foreign exchange may be bought through a currency transfer FinTech, while borrowing and lending may be conducted through crowdfunding or peer-to-peer services. This increased use of specialist service providers means that customers are being on-boarded more frequently, and in an environment where customer experience is increasingly important for competition, time-consuming on-boarding processes are not commercially viable. Both FinTechs and banks now look for fast and simple methods of taking on their customers while complying with their legal and regulatory obligations in relation to financial crime and fraud prevention.

Organisations are applying a more varied range of on-boarding controls. While some request information directly from customers, others utilise information provided by third parties including Facebook and Google. The use of new methods of electronic identification and verification including selfie images, videos and data from third party information providers is becoming commonplace.

But as the number of players and methods of verification proliferate, levels of inefficiency and inconsistency have also increased. Requests for customer data are now duplicated across multiple organisations as individual customers contract with a larger pool of service providers, an inherently inefficient practice. At the same time regulatory guidance is interpreted in different ways by different organisations, leading to an increased risk that in the market as a whole, the overall levels of compliance are reduced and an uneven playing field develops.

Who are the FinTechs?
FinTechs are not a single breed of provider. What they have in common is that they offer services empowered by digital online technology and operate without many of the costs of a traditional retail network such as, bricks and mortar stores, front-line staff or legacy IT systems.

They include challenger **banking service** providers, such as Monzo, Starling and Curve, companies where mobile apps largely replace the physical bank branch. They also include **payment processing** services; these may be retail offerings such as PayPal and Apple Pay, or merchant services such as Stripe. There are also numerous **currency exchange** FinTechs such as Transferwise and Currency Cloud, as well as **crowdfunding** and **peer-to-peer (P2P) lending** providers – some of which also act as payment services providers.

The world of FinTech start-ups is crowded thanks to low barriers to entry, and low operational costs, but do they also carry new financial crime risks? Major banks are able to draw upon mature and tested controls in both customer on-boarding and transaction monitoring, and FinTechs would be required to have similar capabilities. This presents an opportunity for banks and FinTechs to collaborate to address this potential risk.

Reducing market wide inefficiencies without compromising the quality of customer information collected will be critical

Emerging risks II
New products and services

New products are emerging that introduce new financial crime risks.

The rise of new services such as crowdfunding and P2P lending is introducing new financial crime risks to which traditional models were less exposed.

Crowdfunding platforms bring a wide range of investors together with projects that require funding; typically they offer attractive returns including returns in kind, but they also bring higher risk for lenders as these services are delivered by non-banks under less direct regulatory scrutiny than traditional banks. The global nature of these platforms and the relatively high volumes of lending opportunities mean organisations are less likely to be able to conduct 'know your customer' (KYC) controls on their users to the same extent as traditional banks. This opens the possibility of legitimate funding being channelled into misleading or fraudulent investments, or the use of legitimate projects as money-laundering vehicles.

P2P lending also provides a non-traditional platform for individuals to lend money to others and redeem it with interest on expiry of the loan. There are many clear consumer benefits to P2P lending, such as bringing credit services to those who might otherwise be overlooked by the banking sector and offering favourable rates of return to those willing to provide loan capital and bear risk. But, as with crowdfunding risks arise from the global, multi-jurisdictional scale and a lack of rigorous controls.

For banks, there are competitive threats from alternative lenders, but also operational challenges. Some banks are struggling to work out how to risk-assess the providers of such new and innovative services, who themselves require banking services to operate. In some cases, these providers are similar to money service bureaus, which are typically treated as carrying high anti-money laundering (AML) risk. Neither banks nor regulators have been able to develop a clear approach to dealing with alternative lender risks, not least due to the rate at which new lenders are entering the market.

As part of product development, all associated financial crime risks must be assessed and managed prior to launch

Emerging risks III
The rise of cryptocurrencies

Cryptocurrencies pose significant risk management threats to incumbent banks.

New cryptographic techniques have given rise to a new class of currencies called cryptocurrencies. These currencies are based on an approach in which a 'blockchain' of transaction records is stored on a globally decentralised non-bank 'ledger'. Cryptocurrencies are traded outside of the traditional banking network, on peer-to-peer marketplaces or online exchanges; their values are not backed by central banks or governments but driven purely by market demand.

Cryptocurrencies explained

Cryptocurrencies use a technology called blockchain that guarantees the authenticity of a transaction and allows a near instantaneous transfer of value at very low cost. A blockchain is a decentralised ledger of transactions which in practice is tamper-evident and unhackable, and which does not require a central settlement utility for payments such as a central bank. Despite being a public ledger, a blockchain does not contain data as to the identity of ownership: transactions are publically visible but anonymous.

Cryptocurrencies pose challenges for both banks and regulators. From the standpoint of regulators, the most obvious targets for regulation are the exchanges that convert cryptocurrencies to and from traditional fiat currency, as well as facilitating trading of cryptocurrencies. For banks, cryptocurrencies and their potential for hiding wealth make a risk assessment of their customers harder. Despite their own experiments with blockchain technologies, many banks are taking a 'safety first' approach to cryptocurriencies by blocking customer transactions that appear to be transfers between fiat currencies and cryptocurrencies – an approach that is neither effective nor viable in the long term as the new currencies gain mainstream acceptance (several large corporations already accept cryptocurrency payments, including Dell, Microsoft and Expedia).

While there is nothing illegal about cryptocurrencies per se, it is possible to buy such currencies with near anonymity using cash or pre-paid cards at unregulated or local exchanges (although a significant proportion of trading of cryptocurrencies takes place on regulated online exchanges that demand higher levels of user verification). Once purchased, the currency can be moved globally; transaction monitoring is possible but ownership remains opaque. Cryptocurrency users can also break a data trail by mixing identifiable and anonymous funds – a readily used method to launder money, known as 'tumbling'.

Furthermore, such currencies are increasingly being used for the exchange of valuable assets, such as diamonds, automobiles and artworks. Items such as these would usually be subject to High Value Dealer regulations (in the UK for example, a trader accepting payments of €10,000 or more in any transaction must register with the tax authorities for supervision under the 2007 Money Laundering Regulations), making them a channel of choice for crime-related transactions.

A new regulatory and commercial approach to cryptocurrencies is clearly needed

Emerging risks IV
Disruption and disaggregation

More providers and more transactions make for higher financial crime risk.

With the number of players providing financial services in the market growing, the proportion of transactions being processed by any individual organisation naturally reduces, while the complexity of end-to-end processing chains increases. As a result of this, individual organisations will have a more limited view of the overall activities of their customers, making it harder to monitor and identify unusual or suspicious behaviour.

At a market level, the disaggregation of transactions across multiple players therefore increases the likelihood of suspicious activity going unnoticed. An individual financial institution is only able to monitor the transactions occurring within its own systems, yet an increasing amount of activity now takes place out of sight, for example through pre-paid cards or niche foreign exchange services. The result is an overall reduction in an organisation's visibility of activity, which can only be addressed through data sharing and collaboration with other players – both banks and FinTechs.

As the market continues to grow in this manner, traditional methods of transaction monitoring may become increasingly ineffective.

Greater collaboration and use of sophisticated analytics will be needed to manage the fragmented financial services market

The Global Laundromat case

The risks created by an absence of a market-wide view of transactions – especially cross-border transactions – were brought into public attention by the *Global Laundromat* case, where a large number of financial institutions were used unwittingly to launder vast amounts of money between various fictitious companies as part of a single global criminal scheme.

The *Global Laundromat* is the name given to a Moldova-based money-laundering scheme in which the proceeds of multiple crimes originating in Russia were moved into legitimate bank accounts and assets in the EU and US. According to the Organized Crime and Corruption Reporting Project (OCCRP) more than $20 billion deriving from import duty evasion, fake invoicing for state contracts and electronic bank theft was successfully recycled from Russian sources into apparently legitimate assets. The scheme used multiple offshore registered companies that fabricated a series of inter-company debts which were authenticated by captive courts, and then paid down using criminal proceeds. The *Global Laundromat* operated until around 2014, and many of the associated companies were not unwound until recently; much of the laundered money has yet to be recovered.

The laundered funds were processed by banks in the US, UK, Germany, France and China, among others; out of all of these only a handful of banks in the US raised concerns about the transactions. Although many factors contributed to this particular case, it seems clear that a broader and more analytical view of transactional activity would have resulted in earlier identification of such patterns of behaviour.

"Banks will have a more limited view of the overall activities of their customers, making it harder to identify unusual or suspicious behaviours."

Clarifying accountability

Governments and regulators have long expected and mandated banks to be the chief implementers of anti-financial crime controls. This focus is understandable: banks have generated revenues through owning direct relationships with their customers, and are experienced in applying rigorous controls given the strict regulatory environment in which they operate.

While regulations are equally applicable to all financial service providers that fall under the remit of the FCA, for reasons of pragmatism, the regulatory scrutiny has tended to be primarily focused on the larger banks given their combined market coverage.

Banks have had little option but to accept these responsibilities; however, as a greater number of competitors emerge it becomes more likely that banks will seek to address this inequity. Changes in market dynamics will blur the lines of accountability as it becomes less clear who 'owns' the customer relationship.

Rigorous financial crime controls are expensive to implement and maintain, and the penalties for failing to comply with them, both financial and reputational, are significant. In a world where the banks enjoy the lion's share of consumer spending, this could be seen as an acceptable cost of doing business. But when profits are eroded by FinTechs that are not subject to the same regulatory scrutiny, banks must inevitably find a way to either reduce their costs or share them across the market.

"When profits are eroded by FinTechs that are not subject to the same regulatory scrutiny, banks must inevitably find a way to either reduce their costs or share them across the market."

How will the industry respond?

The fragmenting market for financial services raises an urgent question as to the best business model for risk management and mitigation. Incumbent banks have traditionally treated risk management as an intrinsically in-house function, an approach that works when a small number of large institutions own customer relationships and have a broad view of customer data. Will that approach continue to work in a fragmenting market?

We see different types of business models emerging in risk management. The choices that individual providers make will determine which of these models becomes dominant.

The service provider model

One potential business model for banks is the utility model, offering core services such as current accounts or payments processing on a utility basis – this is explored in detail in Deloitte's recent paper on Open Banking. One version of the utility model sees banks evolving into utility providers of financial crime risk management services to other market participants. For example, banks could extend their monitoring systems to embrace the transactions of other organisations, performing a standardised and trusted level of KYC controls on customers at the point of on-boarding and screening of all such customers and transactions for a potential sanctions nexus.

Commoditising these activities and providing them as a service could open up new revenue streams and secure a core role for banks, providing recurring revenue in a dynamic and disrupted market.

There would be risks and challenges for banks. Many incumbents face IT challenges, with legacy platforms that are unable to process unstructured big data as effectively as newer systems. Expanding the technological capabilities would be expensive – but it may also be inevitable.

Full implementation of this model would also require the intervention of the regulators to address the personal accountabilities held by senior banking executives. Few executives would take on the expanded accountability for managing risk across the market without sharing some of that burden with other market participants, or at a minimum having mechanisms in place to personally safeguard themselves against liabilities incurred by third parties.

The market-owned model

Can individual banks be expected to develop a comprehensive response to emerging financial crime risk? Do market-wide issues require market-wide solutions? Given the systemic nature of financial crime and its negative consequences, both economic and societal, regulators may mandate a market utility solution.

We suggest that a government-owned utility would not match market needs – not least as it could appear to absolve banks and FinTechs of their existing responsibilities. However, other models, such as those adopted within the UK settlement market, could see a user-owned, user-governed utility that has both a duty and incentive to provide effective, low-cost solutions to the market.

Utility-type services are already being provided by organisations such as KYC.com and Thomson Reuters. But neither has a dominant market position, nor a comprehensive view of the financial landscape, and there is no agreed industry standard that would guarantee a consistent level of compliance. By contrast a mandated utility could perform all the core operational elements of the financial crime risk management lifecycle, including KYC, screening and transaction monitoring.

There are currently moves towards centrally owned models like this, notably with the Monetary Authority of Singapore piloting a KYC utility that uses government issued ID information to build a trusted data source. There are also precedents for the development of market wide data processing capability, for example moves towards UK adoption of Open Banking standards. Nine UK banks have been mandated by the CMA to develop the Application Programming Interface (API) to implement customer data sharing between financial service providers.

A deadline of early 2018 was agreed for the implementation-ready interface that allows customer data sharing and payment initiation by third party providers.

The customer centric model

Identity and verification: The SmartID solution

Are current KYC controls fit for purpose? We suggest this is a risk issue and an important area for review.

Today's KYC controls require customers to provide their personal information to each financial service provider they wish to use. The service provider then assesses and analyses this data, and seeks to maintain it on a regular basis to reconfirm its accuracy and completeness. This is one of the most costly elements of the financial crime control framework, and is often highly inefficient at an institutional level, let alone at a market level.

However, with the advent of distributed data technologies such as blockchain, it is possible to invert this provider-owned model and enable customers to own and maintain their own digital identity. This is the approach of SmartID, Deloitte's blockchain-based identity concept. By giving customers permission-controlled ownership of their digital identity and associated data, as per the upcoming General Data Protection Regulation (GDPR), the customer on-boarding and information management process becomes more efficient, effective and secure. Trusted data is a key asset in managing financial crime risk and is central to this model, which enables users to create and store identity attributes authenticated through sources such as employers, HMRC, DVLA and Companies House.

Through the SmartID concept, service providers would no longer have the burden of individually collecting customer information, and instead be able to use the verified attributes contained in one's digital identity for identification and verification purposes. Changes to the source information, such as a change of address registered on the electoral register, would be automatically verified by the original endorser to enable on-going maintenance of the profile. Unresolvable changes would be flagged automatically to the banks or FinTechs relying on it, materially reducing the cost of on-going maintenance.

And the smart identity can go further: any entity whether an individual or an organisation can be represented in a SmartID, which also has the potential to hold digital assets representing money or physical property, enabling users to complete complex transactions involving the exchange of ownership and other forms of value transfer, all within a single platform.

"Few executives would take on the expanded accountability for managing risk across the market without sharing some of that burden with other market participants."

Strategies for success

The ability of banks and FinTechs to overcome the challenges of managing financial crime risk in a disrupted environment depend on a number of factors, with responsibilities lying with incumbent banks, new entrants and regulatory bodies. For all three, it is time for new approaches.

The role of the regulator

As the market evolves and the outright dominance of a few large banks is diminished, regulators need to establish new methods of monitoring for the larger number of smaller but significant players. Regulators must find a way to rebalance accountability for financial crime risk management, offering incentives and enforcing penalties to all players in the market to drive the desired behaviours. Clear roles and responsibilities must be set out, with a dynamic framework in place to enforce and evolve them in line with market changes.

Regulators must also embrace the challenge of addressing market inefficiencies, finding ways to drive shared ownership of problems and rewarding collaborative and innovative solutions. The financial crime controls themselves should be revisited and challenged: it seems highly unlikely that today's verification and evaluation processes, dependent on manual file review and on-the-spot interventions will be adequate to manage an enlarged and fragmented financial services market.

Collaboration becomes essential

Many of the structural inadequacies of today's financial crime risk management framework arise from the silos in which banks and FinTechs operate, with data gathering and evaluation built for a market where a few large players dominate. By collaborating and sharing intelligence, learnings and data, organisations will be better able to identify the financial crime activities that are endemic in the system. Pooling transactional data would allow for a more holistic view of the market and for maximum value to be extracted from available data. Enabling this sort of collaboration will require leadership and vision from within the industry, as well as the regulatory support necessary to overcome data privacy and jurisdictional regulatory differences.

Providers must play to their strengths

Banks and FinTechs typically operate under different corporate governance regimes with different levels of risk appetite and different organisational cultures. The platforms that their systems are built upon vary from legacy patchworks built up over time, through to leading edge technologies supported by powerful analytics engines. Banks are most likely to employ experts in banking business lines, while FinTechs are rich in digital scientists. Both banks and FinTechs need to harness industry expertise and experience in financial crime risk management and compliance, and combine this with innovative technology and data analytics to address customer and market problems. But they need to do this by collaborating around their individual skills and experience to develop new approaches to managing financial crime risks.

> "Both banks and FinTechs need to harness industry expertise and experience in financial crime risk management and compliance, and combine it with innovative technology and data analytics to address customer and market problems."

Conclusion

The financial services industry is changing rapidly, with potentially radical implications for the future of banking. With these changes come new financial crime risks arising from the products and services, technologies and new business models required to service a new generation of tech-enabled consumers. Fresh approaches are required to address these risks.

The costs of managing financial crime risks are significant for individual organisations, and at a market level the increasing extent of duplication in certain activities such as KYC introduces costly inefficiencies. To expect banks to continue to bear the burden of what is increasingly becoming a market-wide challenge would place an even greater strain on their already pressured business models, while the evolving FinTechs benefit from avoiding these costs.

A proactive correction to this model is required to address perceived inequities in the level of scrutiny applied to large banks compared to other players, shifting towards one in which responsibility rests on the shoulders of all players in the market, including regulators. But it remains the case that banks and FinTechs alike have a responsibility to address the growing problem of financial crime. However, disruption in the financial services industry may lead to their current efforts becoming less effective.

The changing dynamics in financial services demand a new approach to financial crime risk management that embraces the best of the changes that are already visible within the market. Collaboration, new technology implementation, and an understanding of the shift towards open banking practices and data sharing will be part of the solution. But financial services providers will first need to understand that the fragmented market poses risks that they have not faced before, risks that demand a new category of response that works in a market that has already changed dramatically, and will change further.

Contacts

Andrew Robinson
Partner
+44 (0) 20 7007 0613
andrewrobinson@deloitte.co.uk

Derek Ryan
Partner
+44 (0) 20 7007 8277
derekryan@deloitte.co.uk

Dan Apple
Director
+44 (0) 20 7007 4487
dapple@deloitte.co.uk

Del Nadarajah
Director
+44 (0) 20 7007 2740
dnadarajah@deloitte.co.uk

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J13784