TheCityUK

Deloitte.

Santander

SPLITTING THE BILL

The role for shared platforms in financial services regulation

November 2018

@thecityuk www.thecityuk.com

About TheCityUK

TheCityUK is the industry-led body representing UK-based financial and related professional services. In the UK, across Europe and globally, we promote policies that drive competitiveness, support job creation and ensure long-term economic growth. The industry contributes 10% of the UK's total economic output and employs 2.3 million people, with two thirds of these jobs outside London. It is the largest tax payer, the biggest exporting industry and generates a trade surplus greater than all other net exporting industries combined.

About Deloitte

Deloitte has an unparalleled breadth and depth of services, which make it a world force in its chosen areas of business – audit, tax, consulting, risk and financial advisory. As a leading business advisory firm in the UK, we are renowned for our commitment to innovation, quality, client service excellence and for the calibre of our people.

We serve many of the UK's leading Financial Services firms, providing insightful and impartial advice on how to attract and retain customers to achieve profitable growth. By harnessing talent and expertise across the firm, we deliver solutions to clients that inspire confidence in what we promise. Visit Deloitte.co.uk/FS to discover our latest insights and analysis.

About Santander UK

Santander UK is a financial services provider in the UK that offers a wide range of personal and commercial financial products and services. It has brought real competition to the UK, through its innovative products for retawwil customers and relationship banking model for UK SMEs. At 30 June 2018, the bank has c24,200 employees. It serves around 15 million active customers, via a nationwide branch network, telephone, mobile and online banking; and 64 regional Corporate Business Centres. Santander UK is subject to the full supervision of the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) in the UK. Santander UK plc customers are protected by the Financial Services Compensation Scheme (FSCS) in the UK.

About Clifford Chance

Clifford Chance is one of the world's pre-eminent law firms with significant depth and range of resources across five continents. As a single, fully integrated global partnership, we pride ourselves on our approachable, collegial and team-based way of working. We always strive to exceed the expectations of our clients, which include corporates from all commercial and industrial sectors, governments, regulators, trade bodies and not-for-profit organisations. We provide them with the highest-quality advice and legal insight, which combines the firm's global standards with in-depth local expertise. For more information, please see www.cliffordchance.com and www.linkedin.com/company/clifford-chance-llp.

CONTENTS

FOREWORD

By 2025, financial services providers and their customers will be facing a set of challenges which are in many cases new and diverse. From the mass increase in online data, to the threat of cybercrime, and the demand by clients for a tailored and immediate service, the digitalisation of the market will drive change at an unprecedented pace. The impact on the resourcing and capabilities of both regulators and firms will be substantial.

Responding to these challenges will demand a range of new and innovative technologies and a forward looking regulatory environment which facilitates their adoption and ongoing development. In some cases, prototypes of key technologies already exist, ready for deployment in a market which is yet to catch up. At times these barriers to adoption may be legal or regulatory; in other cases it is the need for industry buy-in at scale, with competitive pressures pulling in the other direction.

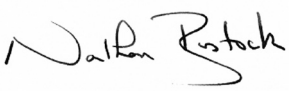
It is clear that a collaborative approach based on partnership between industry, government and regulators will be key. This paper reinforces how collective participation in digital platforms, which are recognised by the regulator, will bring about a range of strategic benefits including greater transparency, a more resilient market and robust consumer protections. For the firms who engage there will also be increased efficiencies in process and reductions in cost. There will also be direct benefits for consumers who will find it easier and quicker to apply for new financial products, and to switch their accounts to more competitive providers.

The outline of shared platforms for Know Your Customer (KYC) and regulatory reporting, as developed by Deloitte in this paper, is part of ongoing work for HM Treasury's Financial Services Trade and Investment Board (FSTIB). As highlighted in the government's FinTech Sector Strategy, the approach could be extended to cover a wide range of additional activities including collateral management, fraud management, loans processing, trade finance, identity management, and transaction monitoring.

This report and the recommendations outlined within, particularly around liability and securing a critical mass of industry participation, will accelerate progress in this field. The high number of related initiatives and pilots underline the level of appetite for progress. We look forward to continuing our work with HM Government and developing an environment which enables the many benefits of shared platforms to be realised. If the UK is to retain its reputation as a leading market for FinTech innovation it is critical that we secure progress in the short term; already many international competitors have caught up with UK's achievements to date.

This report has been made possible with input from across the UK-based financial and related professional services industry and we would like to thank everyone who has contributed, in particular the team from Deloitte and also Clifford Chance who have assisted with the work on liability.

Miles Celic
Chief Executive Officer,
TheCityUK



Nathan Bostock
Chief Executive Officer,
Santander UK

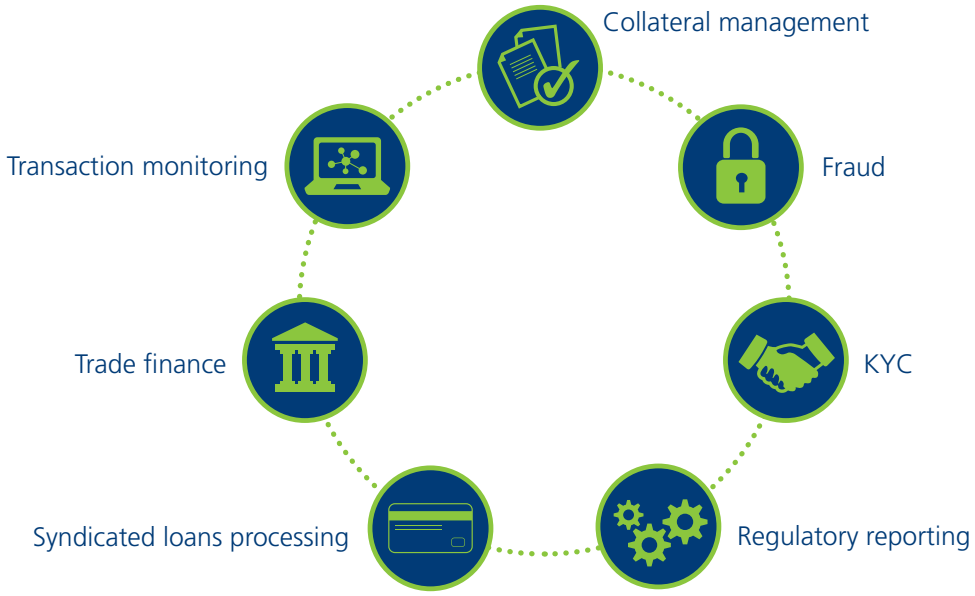
Louise Brett
Partner and FinTech leader,
Deloitte North West Europe

EXECUTIVE SUMMARY

The purpose of this paper, commissioned by the Financial Services Trade and Investment Board (FSTIB), is to explore the hypothesis that the creation and widespread adoption of shared platforms across the financial services sector will result in improved efficiency of compliance, reduced operational costs and improved customer experience. A further consideration is whether shared platforms, in effect digitally-based utilities acting as a service provider for certain regulatory activities, will facilitate easier access to services for existing and new market entrants with an overall net positive economic effect. In the context of the discussion presented here, a shared platform refers to a combination of technology, process, controls and policies and is not intended to refer solely to a technology solution or advocate one technology approach over another.

Shared platforms

This report identifies seven shared platforms. These include:



Two shared platforms, Know Your Customer (KYC) functions and regulatory reporting, were identified as the two concepts to investigate further on the basis of the potential benefits (for industry and society) and the current momentum for change. These are explored in more depth on pages 24-44.

The objective was to examine the concept of these shared platforms in more detail and, from that, define clear next steps and recommendations for government, industry and the regulators that would support the practical realisation of these shared platform concepts.

The cases that we have included each carry significant merit and, in many instances, the ideas are not new, albeit they remain some way from reaching full scale adoption. The concept of shared platforms has increasingly been receiving global attention, with the World Economic Forum (WEF) explicitly listing shared solutions to common problems as one of its key findings.[1]

In each of the opportunities explored in this paper, there is significant benefit to be had by UK financial services firms and the economy, especially if we can export and implement these ideas on a global basis.

[1] World Economic Forum, 'The new physics of financial services – How artificial intelligence is transforming the financial ecosystem', (15 August 2018), available at: https://www.weforum.org/reports/the-new-physics-of-financial-services-how-artificial-intelligence-is-transforming-the-financial-ecosystem

Anticipated benefits of shared platforms

- **Delivering on strategic objectives:** shared platforms could provide greater transparency and auditability of activities, driving a step change in delivering strategic objectives and societal benefits such as the identification and prevention of fraudulent activity and reduction of financial crime.
- **Improved customer experience:** improved processing times, operational efficiency and flexibility – improving the overall customer experience and facilitating greater competition in the industry by making it simpler and quicker for consumers to switch providers and secure new financial products.
- **Exporting UK tech expertise:** each of the shared platforms could be replicated in other markets, presenting the UK economy with an effective export of its expertise in FinTech innovation.
- **Cost reduction:** reduction in operational and administrative overheads and associated costs for individual institutions by adopting a shared platform approach – reducing the risk of ever increasing costs which can be passed on to the customer.
- **Standardisation:** greater standardisation and consistency across the industry through the use of common standards, protocols and services, while being careful not to stifle innovation.

Summary of shared platforms recommendations

In recent years the financial services sector has demonstrated an appetite to embrace new technologies and regulation through initiatives such as Open Banking and an increasingly collaborative environment. However, while support for the concept of shared platforms remains strong and the benefits clear, challenges and impediments remain and continue to limit the ability to develop these concepts into fully operational solutions, namely:

- **Liability and accountability:** the senior management arrangements are well understood and provide clear lines of liability back to individuals and organisations. The move to shared platform services goes hand in hand with a need to reassess risk appetite for outputs from such platforms. This will require government and regulators to consider how liability and potential penalties should be apportioned and to define protocols and processes for a model where organisations are working with, and are reliant upon, third parties and shared services.
- **Regulatory alignment:** government will need to work with its counterparts to align on regulatory frameworks and policies to enable global organisations to use these shared platforms in an interoperable way across geographies and jurisdictions. The current drive to build national utilities may serve domestic markets, but could also increase global fragmentation.
- **Technology:** industry participants, and the third parties that supply them, will need to define common technology protocols and solutions to aid ease of adoption and operation and to address the challenges associated with keeping information on shared platforms current in a fast moving environment.
- **Data sharing:** the regulator and the Information Commissioner's Office should consider an approach to promote ease of data sharing within the constraints of existing privacy and banking secrecy protocols.
- **Identity:** the ability to unequivocally confirm the identity of an individual or organisation is becoming increasingly important. The concept of a Digital ID may address this but that comes with societal challenges. The government should support the drive towards Digital ID, drawing on the range of benefits for the individual, the enterprise and society.
- **Adoption:** success requires material uptake/adoption by the industry and customers, with customer experience and financial inclusion needing to be front of mind. The move to shared platform models requires a longevity of objective which requires sponsorship at both the Board and Executive level.

As noted previously, KYC functions and regulatory reporting were identified as two concepts to investigate further on the basis of the potential benefits (for industry and society) and the current momentum for change. See below specific recommendations for each area. These are explored in more detail further in the report.

Recommendations for Know Your Customer (KYC)

- **Accountability and liability:** government and the regulator should explore options in conjunction with industry around how the regulatory framework should be adapted for a shared platform model.
- **Clarity of requirement:** the shared platform solution should be underpinned by a focus on defining central policies and common standards for data collection and assessment.
- **Data sharing:** government and industry should work together on identifying and driving toward the most pragmatic solution to make data sharing as efficient as possible.
- **Trusted sources of data:** agreement needs to be reached between regulators at a regional, and ultimately, a global level on data standards and the provenance of data into and out of the shared platform.
- **Identity and security:** government should consider the drive towards digital identification at scale as a strategic objective.
- **Market participation:** starting at the regional utility level, regulators in collaboration with industry should work to define a set of common standards (technical, data and process).
- **Ownership, operational and commercial models:** establish a working group to look at the ownership, target operating and commercial models. Current activity in the market show that some form of consortium approach, either between banks or involving a third party, has some momentum already.
- **Regulatory alignment:** government should promote UK prototypes/experiences in global fora and in the Financial Conduct Authority's (FCA) Global Financial Innovation Network to move the wider industry towards regulatory alignment wherever practical.

Recommendations for regulatory reporting

- **Clarity of requirement:** regulators need to define their data requirements more clearly and coordinate their data requirements with each other. Regulators should take the lead on developing new solutions and approaches to enable the definition and communication of regulatory requirements in a way that removes interpretation and scope for ambiguity. The industry will need to address the common challenges around data quality and consistency of standards within and between organisations.
- **Accountability and liability:** government and the regulator should explore options in conjunction with industry around how the regulatory framework should be adapted for a shared platform model.
- **Collaboration:** a culture change, led from the top, is required to promote collaborative ways of working.
- **Precedent:** continue with the proof of concept approach, while considering these can be scaled up for mass production.
- **Commercial models:** establish a working group to look at the target operating and commercial models.
- **Appetite for change:** articulate a clear benefits case, as well as broader incentives for adopting a shared platform solution.

We recognise that the regulatory landscape, particularly cross border, has evolved over a number of years and has involved detailed and carefully managed negotiation. Early engagement with government and the regulators in exploring and taking forward the recommendations presented in this paper will be essential so the broader sensitivities and priorities can be addressed appropriately. While the long term aim should be a merging of shared platform initiatives cross border, with the US in particular, the UK should take confidence from its status as a leading global hub and the international appeal that exists for the initiatives we shape and drive. Failure to tackle these issues could harm the competitiveness of the UK given the pace of innovation across international markets. A number of other jurisdictions have already edged ahead in this field.

Technology has driven the core of financial services for many years. We believe the UK is well placed to leverage its position and understanding of financial markets, its FinTech leadership and regulatory preeminence to drive innovation in the market for years to come. The positive approach that has placed the UK at the forefront of the FinTech revolution benefits start-ups, incumbents and consumers alike, but to capitalise further requires start-ups and incumbents to better understand how to approach and work with one another. This is discussed in more detail in the 2017 report 'Transformation and Innovation: a guide to partnerships between financial services institutions and FinTechs' published by TheCityUK, with support from Santander and Shearman & Sterling.

It is also important to recognise that the successful adoption of shared platform models goes far beyond technology. It is often the legal, regulatory and societal dimensions of a shared platform model that pose the greatest challenge.

Shared platforms are the next frontier for the transformation of financial services and, building on the UK's already strong position, we look to government, industry and the regulators to work together to address the opportunities and challenges presented in this paper.

THE CONCEPT OF SHARED PLATFORMS

Introduction

There is a commonly-held belief that there are opportunities within the financial services sector to improve compliance, reduce costs, increase competition and deliver better customer outcomes through the implementation of industry wide standardised services. This is especially the case given when these activities do not provide a competitive advantage for incumbents and are currently carried out internally, with financial services companies and markets duplicating the work of each other. Shared platforms also provide a mechanism to support the delivery of significant strategic objectives for government around fraud and financial crime.

This paper identifies and articulates the benefits of, and potential for, the creation of FinTech-related financial services shared platforms in the UK.

Principles

To qualify as a potential shared platform, we have identified a number of key principles that an opportunity must satisfy:

- The service would provide a demonstrable benefit to multiple parties in the financial services sector and promote positive consumer/customer outcomes.
- Delivery of the service would not impact upon an industry participant's competitive advantage relative to other industry participants.
- The service could be delivered as a shared platform – it is a repeatable activity, with a consistent outcome, that can be clearly defined, measured and commercialised.
- The new service, or combination of existing services into a platform, is not already being provided by an industry incumbent to the extent that would be provided by a fully shared platform. Existing services would be regarded as out of scope – the focus of this paper is not to create new competition for existing service providers. However, we acknowledge that there may well be start-ups or incumbents that have plans to target some of these areas. We have only considered those that are already in the mainstream of the industry.
- Current legal or regulatory limitations to the implementation of the platform can be revisited and need not be an immediate blocker.
- The potential to maintain or improve the competitiveness of the UK.
- The solution should be institution or vendor agnostic and promote the use of open architectures and common standards so as not to artificially create a commercial advantage for one vendor or institution over another. There are a number of industry and government pilot projects underway, so it is appropriate that we discuss and draw lessons from these as part of the options analysis and recommendations.

As an example of the above, and in respect to the final point, it has been argued that the UK should look to implement a new, modern, set of Payment Rails to support the future needs of financial services, both within and beyond the UK. The central UK payments bodies are already working to achieve this, and are developing a strategy for future development. Consequently, coverage of a new payments platform for the UK was excluded from this analysis.

Analysis of the market opportunity

While we identified more than a dozen shared platform opportunities, a number of them did not satisfy the criteria above. Consequently, our shortlist was narrowed down to seven. These shared platforms include: collateral management, fraud, KYC, regulatory reporting, loans processing, trade finance and transaction monitoring.

We have identified a number of benefits and constraints for each of the shared platforms, such as improved speed and efficiency. Although a shared platform does not necessarily need all market participants to buy into it in order to be commercially viable, the more organisations that engage, the more economical it will become and the greater the benefit it will generate for participants.

Potential shared platforms

The following chapter will outline the following potential shared platforms:

Collateral management – providing a central repository for tracking all collateral used for financing

Description

Currently there is no central database of collateral tracking information. This is operationally challenging and presents issues to clients in their attempts to meet the requirements of the Client Asset Sourcebook (CASS) with regard to holding client money or assets.

To address this problem, an opportunity exists to create a central repository that tracks collateral used by financial services institutions. By having a central repository, it will make it easier and quicker for institutions to track all charges on collateral and allow them to better assess financing options.

The overriding challenge in making this work will be the level of trust that organisations can place in the information on the central repository and the position on liability should this information be used in good faith but prove to be incorrect.

The potential to extend this by physically taking the security at the outset was considered and parked, recognising that different banks will have varying levels of commercial appetite for this.

A shared repository would mean that:

- Financial services organisations will only need to go to one platform to understand any specific assets and charges.
- It will be very quick and easy to understand any current charges on the asset.
- There is potential scope to derive considerable benefit for automation of secured lending (refinancing).
- There is a potential wider benefit to promote the switching of customers and the use of No Search Indemnity Policies in order to mitigate the cost and time involved in refinancing.
- The use of new technology to reduce the number of intermediaries and hence improve the efficiency and speed of transactions.

Key activities

The collateral repository platform would be responsible for the following activities:

- Ensuring that all collateral that has been financed is entered into the repository, including expiry date and terms and conditions. This may also need to include historical data.
- Providing asset value and charges by institution and by level of charge (1st charge, 2nd charge, etc.).
- Validation of charges against government ledgers where such data exists, for example Companies House in the UK.

Fraud shared platform – monitoring, identifying, tracking and reporting fraud and attempted fraud

Description

Fraud, in the context of the illegal obtaining and distribution of funds, is a common problem across the financial services sector. While some sharing of data occurs, there are many instances of fraud that are not shared, or are not even appropriately identified due to their distributed and/or low level nature. Additionally, there are many instances of fraud carried out through deception against customers.

According to the ONS there were over 3.3 million reported cases of fraud in 2016, with 2.5 million of those related to bank and credit card fraud.[2] From a consumer perspective, it is estimated that fraud impacts almost 1 million people in the UK each year, and costs the public more than £300m. The cost to the industry is not known, but it is clear that even if it were calculated, the figure would remain low as a lot of fraud goes undetected or unreported.

Fraud covers a multitude of different crimes and such a fraud platform would need to cover as many of these as possible, including both physical and digital fraud. With the growing level of digital/electronic fraud, it is likely that much of the focus of the platform will be on digital/cyber fraud in the coming years.

Currently, financial institutions are required to report fraud to the National Crime Agency and the UK government has established Action Fraud as a central, UK, anti-fraud function to allow customers to do the same. Organisations such as CIFAS have also been established to support fraud prevention. However, there are challenges with moving this from simply fraud reporting and analytics to actually being able to drive real-time action and intervention. As a global industry, which is increasingly reliant on digital technologies, a more sophisticated, industry-funded, platform could provide a focused 'real time' fraud response and communication facility.

[2] Office for National Statistics, 'Crime in England and Wales: statistics bulletin', (year ending December 2017), available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2017

A shared platform would provide:

- A central repository of known fraudulent activity that can be used by industry participants to help identify and protect against fraud.
- A centre of excellence for defining good practice in anti-fraud measures that can be provided to industry participants.
- A mechanism for identifying and providing a coordinated response to fraud carried out on a grand scale by, for example, sophisticated cartels. The 'money mule' analysis work performed by Vocalink for MasterCard is a good example.
- A voice of the industry for communicating fraud activities to the public and assisting in ensuring the public is best prepared to defend themselves against such attacks.

Key activities

The fraud shared platform would be responsible for carrying out the following activities:

- Working with financial services organisations, the National Crime Agency and Action Fraud to define and implement best-practice anti-fraud measures throughout the industry.
- Providing training and communications to industry participants.
- Tracking transactional data centrally in order to spot fraud perpetrated through distributed events across multiple banks. This would require market participants to share transactional data and significant real-time or near real-time processing capability in the fraud platform.
- Acting as a central repository for detailing known fraud activities/processes and disseminating this data across the industry so that all participants can protect against it.
- Reporting on fraud to assist the industry in understanding the scale and impact of fraudulent activities as well as tracking progress in fighting fraud.
- Acting as a central point of management to defend against fraud, including providing up-to-the-minute details of fraud attacks to both financial services institutions and customers.
- Issuing communications to the public to warn them of new instances of fraud and how to protect themselves from such attacks.

It should be noted that the shared platform would not be responsible for acting as an arbiter in the event that a customer raises a complaint against an industry participant.

KYC shared platform – providing KYC functions and acting as a central repository for identified entities

Description

KYC activities must be carried out by financial services organisations before they can take on customers. In many cases KYC can be a manual and intensive process and for customers that are shopping around for services, or who have complex requirements, the process may need to be carried out by many potential providers, which can be time consuming. KYC is particularly important for the industry, to combat money laundering and terrorist financing, but is often slow and frustrating from a customer perspective.

There is already some very interesting activity in the market regarding KYC:

- Five of the biggest banks in the Nordics are working together to explore the creation of a joint anti-money laundering solution, which would incorporate KYC. This would serve the five sponsoring banks and also be open to third parties to use for a fee. The shared utility is scheduled to launch in the latter part of 2018 pending approval from the EU competition authorities. The initial focus will be corporate customers, with the potential to expand to retail customers in the future. It is not clear at this stage how, or indeed if, any risk transfer or shared liability concepts are integral to the proposed operating model.
- Recently, HSBC has agreed to sell its new compliance system, which performs automated checks on clients through a deal with a third party. These checks cover both corporate and institutional clients and the intention is to offer this more widely as a service to rival banks.

Fundamentally as a concept, a shared platform for KYC would provide:

- A common, central service for KYC, reducing administrative overheads, on-boarding timeframes and the risks of misidentification or KYC failures due to use of different data sources.
- Reduction in the need for in-house staff to complete KYC.
- Coordinated tracking of identities.
- The potential to extend the service across a broader set of geographies, subject to regulatory approval.
- Support for the drive to increase competition in the market by allowing smaller-scale organisations to access KYC services on a transactional basis.
- Potential for organisations to utilise KYC checks previously performed by other organisations rather than performing the same checks again.

Key activities

The KYC shared platform would be responsible for carrying out the following activities:

- Personal KYC: KYC for individuals, including the collection of any required documentary inputs, biometric data and analysis of this data to confirm identity, check criminal status and immigration records and identify any potential risk of fraudulent applications.
- Corporate/multi-party KYC: completion of KYC for multi-entity parties, for example SMEs, corporates, charities and trusts, including personal KYC for specific individuals, ultimate controlling entities etc.
- Storage of KYC results: once KYC has been completed, the record will be stored for use as the basis of future KYC requests.
- Ongoing management of KYC records: periodic review of KYC entries to re-confirm that the data is valid and/or updated when notified of changes.

It should be noted that there are a range of potential operating models for KYC which we will consider later in this paper.

Regulatory reporting – improving the ease and consistency of regulatory reporting

Description

Regulatory reporting is a vital activity that all regulated financial services organisations have to carry out to ensure compliance. With the majority of reporting still carried out manually, this can more often than not be a slow and error-prone process.

While the reporting requirements specified by regulators may be intentionally broad so as not to constrain the response, this can lead to misinterpretation or misalignment with the regulator, leading to rounds of follow up and clarification. For example, with CoRep (Common Reporting Framework) and FinRep (financial reporting) there are a range of assumptions and documentation regarding how banks have interpreted the rules. There is also a challenge with the variation in data quality and standards across the industry and a sense that multiple similar, but not quite identical, requirements further add to the reporting burden.

As regulations continue to increase and new standards are introduced, the scope of regulatory reporting is increasing. Financial services organisations will benefit enormously from a shared platform on which regulatory reporting is clearly defined and standardised and can be automated, allowing for real-time responses to the regulator. Any solution should seek to utilise modern developments in artificial intelligence and self-learning algorithms in order to automate, improve accuracy and reduce costs on an ongoing basis, while also addressing the requirements of privacy and banking confidentiality.

In considering regulatory reporting, there are two approaches that have been considered: a centralised regulatory reporting platform and a common distributed ledger based solution. Both look to reduce the administrative burden and improve consistency and clarity.

Key activities

A centralised regulatory reporting shared platform would mean that:

- Financial institutions only need to go to one platform to understand any regulatory changes, and gather best practices for regulatory reporting. This would allow these institutions to take a proactive approach to regulation, rather than a reactive one – allowing them to forecast and build strategies in line with regulatory changes.
- Auditability and traceability will be enhanced ensuring that financial services organisations are being compliant.
- A consistent approach is taken to the creation of regulatory reports, providing standardised asks and outputs and dealing consistently with data.
- The ability to deal with growing regulatory demands efficiently in a fully industrialised fashion, including handling ad hoc requests from the regulators.

Syndicated loans processing – providing a central platform of the processing of loans

Description

Loans are one of the most common products that financial services institutions offer to their customers. However, the complete process from the origination and disbursement of a loan, to the servicing of it can be an expensive and arduous process – particularly if the loan is syndicated.

Currently, syndicated loans are booked on a financial services institution's internal platform, with settlement periods taking up to three weeks. A future solution is to have a central platform for the processing of the whole lifecycle of a syndicated loan. By having a central platform, the lending process can be streamlined, helping untie capital for the sell-side and giving certainty to the buy-side.

Readers should be aware that steps are being taken forward to create a blockchain based syndicated loans processing solution by Ipreo and Symbiont in conjunction with a number of market participants.[3]

A shared loans processing platform would provide the following benefits:

- As an automated and digital system there will be no need for a paper-intensive loans process.
- A consistent provision of loans, providing transparency and efficiency across the market.
- Reduce loans settlement times and eliminate costs for each participant to maintain internal lending systems, encouraging more lending. A reduction of the cost per loan frees up capital on the balance sheet to enable further lending.
- A more cost effective solution for new market entrants.

Key activities

The syndicated loans processing platform would be responsible for carrying out the following activities:

- Working with financial services organisations to define and implement best practice loans processing measures throughout the industry.
- Offering a shared platform for the origination and servicing of syndicated loans.
- Financial services institutions would be able to enter data to originate and settle loans. They would then also be able to settle, trade and make payments on those loans.

[3] IPREO, 'Financial institutions move closer to realizing a blockchain solution for syndicated loans', (30 March 2017), available at: https://ipreo.com/press-releases/financial-institutions-move-closer-to-realizing-a-blockchain-solution-for-syndicated-loans/

Trade finance – providing a central repository of all trade finance transactions

Description

Historically, trade finance transactions are fragmented and difficult for financial institutions to track and easily engage with one another. It can be a paper-intensive process when you consider everything from packing lists and inventories through to invoices and certificates of insurance. An average trade transaction requires around 65 data fields to be extracted from 15 different documents spanning 40 pages.

There would be significant benefit in being able to automate the processing and sharing of documentation and transaction details, and this is where new technology and protocols could be beneficial.

A shared platform would provide the following benefits:

- faster, more efficient way of collecting and sharing the significant volume of paperwork associated with trade finance transactions
- consistent view to allow all banks to understand trade finance transactions
- enabling of financial services organisations to assess risk with specific transactions
- increased transparency and trust among all players.

It should be noted that approaches to streamlining trade finance transactions are currently being developed in the market. For example:

- One global bank is applying optical character recognition and cognitive technology to automate the processing of paper documentation in trade finance transactions.
- Vendor offerings are coming to the market that reduce the process overhead and need for human intervention, using blockchain technology to reduce the number of intermediate parties involved in a transaction and reduce risk.
- Recently, Currenxie launched a trade finance solution for Amazon sellers, allowing them to apply for financing linked to a real time global collections and payments platform. This allows the seller to draw on liquidity tailored to their needs.

Key activities

The trade finance repository platform would be responsible for ensuring that all trade finance transactions are documented and therefore easily allow financial institutions to communicate and transact with one another based on the information on the platform. New technologies can also improve processing time and reduce risk through improved transparency, access to information and the reduction in the number of intermediaries involved.

Transaction monitoring shared platform – a centralised global transaction monitoring solution

Description

The global financial services sector processes billions of pounds of transactions on a daily basis. Much of this is high frequency and low value, but there is also a substantial quantity of higher value transactions. Currently, individual financial services businesses are responsible for monitoring their own transactions to identify fraudulent or suspicious activity. While this is moderately effective it leaves the system open to abuse by rogue states and organised crime through the funnelling of payments through multiple financial services actors. Often, such dubious transactional activity is only identified sometime after the fact when it is too late to stop the activity.

A shared platform would provide the following benefits:

- A centralised platform for identifying and providing a coordinated response, particularly when this is perpetrated against a number of actors in a coordinated fashion in order to avoid detection through conventional means.
- A central repository of known suspicious activity that can be used by industry participants to help identify and protect against both ongoing and future instances.
- Improved intelligence and data analysis that improves the chances of being able to repatriate any misappropriated funds.

Key activities

The transaction monitoring shared platform would be responsible for carrying out the following activities:

- gathering transactional data from market actors, including tracking transactional activity that occurs across multiple parties
- monitoring the data in real-time or near real-time to identify suspicious activity
- alerting participants, regulators and law enforcement agencies to emerging patterns of suspicious activity
- gathering data on suspicious activities and reporting upon them
- sharing data with regulators and law enforcement agencies
- providing guidance on support to market actors in establishing more capable transactional monitoring functions in-house.

The concept of a centralised transaction monitoring repository is not new. The challenge to date has been twofold:

- The ownership and funding model for such a platform has not been defined. This may, for example, need to be run by government and funded by industry but such an arrangement has not been agreed.
- As institutions improve their ability to detect suspicious transactions, they in turn expose themselves to increased penalties as a result if such suspicions are not acted on in a timely manner.

It should be noted that the shared platform would not be responsible for acting as an arbiter in the event that a customer raises a complaint against an industry participant.

Common attributes, challenges and risks of the shared platforms

There are a number of common attributes for each of the shared platforms described, along with a common set of risks and challenges to be addressed.

Impact of market participation on shared platforms

In all cases, the shared platform opportunities identified become more effective as the number of market participants using them increases. In some cases, such as transaction monitoring and collateral management, the implications of low market penetration are much more profound. In these cases the shared platform would be ineffective if critical mass were not achieved and a slow adoption rate could kill such an initiative.

It will be important to conduct a tipping point analysis to better understand the point at which the benefits for the customer, banks, regulators and governments are realised. Implementing local solutions that then scale and expand cross border may make it easier for larger organisations to adopt shared platforms earlier, which in turn drives increased volume and uptake.

To a degree, market participation will go hand in hand with the pace of regulatory alignment and the agreement of standards and controls across jurisdictions. There is significant work required here between governments and regulators. Once that is enabled, then should participation by market participants become an issue, government intervention in terms of either legal or regulatory change might be required. Enforced mandatory adoption would only be needed where the platform is not effective (in terms of its desired benefits) without a large proportion of the market adopting it.

The adoption of shared platform solutions does create questions around how liability and accountability will change as a result. Participants in the shared platform will need to be able to take confidence in its operation and outputs and, if forced adoption were to be mandated, the government or regulator will need to provide a level of reassurance that a participant firm will not be held responsible if the shared platform fails to deliver appropriately (unless the issue is also related to poor management of the supplier by the incumbent).

Data sharing

With the growth of complex data analytics and the development of ever more sophisticated networks, the means to gather, store and query data have become ever more important to modern businesses and the value of that data has increased exponentially. Consequently data, access to data and ownership of data have become progressively more important issues. As such, it should come as no surprise that data related concerns would feature highly in any list of issues related to the development of shared platforms.

By definition, shared platforms are dependent upon data being shared between the participating entities and the shared platform itself. In some cases this may even require data to be shared between the participating entities, either directly or indirectly through the shared platform. The prospect of sharing of both bank and personal data generates a number of potential barriers to establishing, and getting buy in for a shared platform.

It should be noted that the financial services sector is already facing a number of significant changes that have a fundamental impact upon the way that data is managed and shared, these include:

- January 2018: Open Banking required retail banking market participants to provide the facility to share data with, and allow payments to be initiated by third parties.
- May 2018: the General Data Protection Regulation (GDPR) replaced the UK Data Protection Act 1998, bringing into play a number of changes to the way that data is managed, stored and accessed.
- April 2018: the EU Directive on the security of Networks and Information Systems imposes significant new obligations in relation to data security, notification of breaches and compliance, coupled with significant potential fines.

The challenge lies in the current ability to share data between organisations. The effectiveness of shared platforms will be dependent upon the industry and government establishing a more comprehensive position on responsibility for shared data, both in terms of the originating party and the recipient, which could assist in addressing some of the issues identified above. Making it as easy as possible to provide consent for data sharing within the bounds of law and regulation will also support the adoption and success of shared platforms.

Data management

The customer is always the ultimate owner of their own data. However, from a corporate perspective, maintaining responsibility for that data becomes increasingly difficult as it is consumed by the shared platform and then joined with data from other sources in order to either create a composite data set or to support the day-to-day activities of the platform. Legislation such as GDPR will drive improved data integrity and also require that a customer has certain rights that they must be able to invoke through the original recipient of their data. For example, if a customer wishes to be forgotten then they will expect to be able to do this through contacting the organisation that they first gave their data to and have their relationship with, not the shared platform.

The uses for data from any shared platform will therefore need to be carefully defined in the original contract with each participating market entity. In turn, these will need to be 'backed-off' between the market entity and their customers. Where a customer requests for their data to be modified in some way (as a request to forget or for data errors to be rectified for example), this must be enforceable through the market participant / shared platform contract.

This requires that the shared platform must always be able to identify and appropriately manage an individual customer's data, meaning that compound or 'melded' data sets should only be used either where customer data is anonymised, or where the data is only created as a transitory entity.

Where data is owned by market participants themselves, it would seem reasonable that they will expect the use of that data to be tightly governed through the contractual and ongoing service relationship with the shared platform in much the same way as they will manage customer data. There is also the opportunity to potentially have access to data that is not currently available (e.g. registers of beneficial ownership). This presents an opportunity, but also needs to be considered as part of the evolving governance and controls required.

Acting as the provider of a shared platform generates a number of significant data management issues for a business, particularly where that business is entering into a domain where a large amount of data already exists within individual market participant's own systems. KYC services is an excellent example – to provide an effective KYC capability on day one, the shared platform should first start with the data already available in the market, using that as its base data set. However, the ability to share that data is constrained and in most cases matching of data from one market participant to that of another will be a complex activity. Simple differences, such as spelling variations or abbreviations, can complicate matters, as can changes of address or marital circumstances. For the purposes of this document, these issues are regarded as technical challenges that the shared platform will need to devise a method for overcoming. With advances in database and data management/analytics technologies, combined with emerging technologies and protocols regarding biometrically enabled 'digital identity' this should not be impossible.

The greater challenge for the shared platform is data quality and timeliness, particularly where there are errors in the data, either due to errors in data received from market participants, in matching of data from multiple participants, or in errors generated through the activities of the shared platform itself. Where such errors exist, it is possible that incorrect data could impact upon the effectiveness of the shared platform. For example, a fraudulent transaction could pass through unchecked, or a member of the public could be turned down for a mortgage. In such cases, the issues are likely to be somewhat localised, but the impact to the individual or business impacted by the data error could be enormous. Data being current and up to date is key for all of the processes described here which presents a significant maintenance challenge.

Of course, while data errors can result in fraud going unchecked, there are many fraudulent activities that occur every day where the market participants simply fail to spot the activity, or identify it too late to recover the monies involved. Such cases, particularly where they involve small businesses or consumers, commonly appear in the press and highlight how hard it is to get the balance right between the market participant and the end customer taking responsibility for the fraud.

The creation of a shared platform will complicate such matters. Where the market participant firm might ordinarily be expected to identify and stop a fraud, they may now assert that they are handing responsibility for some elements of that process to a third party.

The problem that this generates is that the impact of such issues are likely to be felt by the end customer and, through them, the market participant firm. A means must be found to determine fault, who is responsible and how appropriate recompense is made.

Clarity on the regulatory ask

A common challenge, and one that has arisen frequently when exploring the shared platform concept for KYC and for regulatory reporting, is the benefit that would be derived from increased clarity around the regulatory ask. As it stands, there is a degree of interpretation associated with the requirements, protocols and rules in both of these areas. This leads to an operational overhead due to increased effort to clarify the rules or in multiple iterations of responding due to the original response not being in line with the intent of the ask. This challenge exists at a regional level between regulators and institutions and becomes more complex when you then look to extend cross border.

Security

A shared platform, by definition, will hold data from multiple market participants and in many cases will also hold customer data (either retail or institutional customers). Due to the concentration of data in a single source, the shared platform could be a tempting target for hackers, and the losses associated with any successful attack have the potential to be far reaching in terms of the numbers of end customers impacted.

Ordinarily under such circumstances the Information Commissioner's Office and the FCA would assess the situation and determine an appropriate response and/or action against the firm should it be proven that the data loss event was preventable. This should still be the case with a shared platform, although management will need to be held responsible, in a similar fashion to regulated executives, under the Senior Management Regime or equivalent.

Governance

Under the FCA Senior Management Arrangements, Systems and Controls (SYSC) guidance firms are held responsible for managing activities of their outsourced service providers carried out on behalf of the firm. When a firm outsources an activity it must be able to prove that it has the skills, experience and processes in place to assess, contract with and manage the ongoing service provision of that outsourcer.

As part of this ongoing engagement, the firm must ensure that it provide appropriate oversight and management of the activities of the outsourcer in relation to the outsourced functions. In the event of a failure of that outsourcer in carrying out its duties, the firm can be held responsible and action taken against the firm and individuals within that firm.

In the event that a mandated shared platform is implemented, this creates an issue for the firm. Having no choice in selecting its outsource provider, the firm is limited in its ability to comprehensively meet all of its obligations under SYSC 8 and 13.

Under the circumstances outlined above it would seem reasonable that the industry and the regulator should agree which elements of SYSC guidance need to be adjusted (either generally or in specific reference to the mandated services) to ensure that individual participating firms are not unduly penalised for a failure. This is not to say that firms should not be expected to manage and oversee their relationship with the shared platform, merely that consideration should be given to how such a mandated relationship should be managed under the SYSC guidance.

Accountability and liability

There is a fundamental question to address around where accountability resides with the use of shared platform solutions. Currently a senior executive in a financial institution is accountable should there be issues, for example, with KYC. In a shared platform solution with a degree of delegated responsibility, the position on ultimate accountability needs to be considered.

A shared function, be it for KYC checks or for fraud monitoring, could provide industry participants with a false sense of security, thereby leading them to believe that they do not need to manage this as robustly as today.

The shared platform could also be at risk of being held liable if it fails to spot fraudulent activities. This would be of particular risk if industry participants lost large sums of money to a coordinated fraud attack that the centralised shared platform was late to identify.

The ultimate solution may be to move to a point where the platform itself is regulated, thereby allowing institutions that use that platform to take confidence in the output. However, no regulator has to date expressed an intention to regulate such a platform or to accept the additional responsibility that would place upon them. In the event the utility does become a regulated entity, and itself liable for any regulatory breaches which might occur, firms would have to undertake exit planning to cover the possibility of the platform going insolvent due to the claims against it.

In reality, the solution is likely to be a more gradual, progressive approach in terms of how liability and accountability may evolve. Within the industry currently, the concept of risk transfer does not exist; an organisation can outsource operational functions, but accountability at this regulatory level remains with the institution. This suggests that as things stand, a shared platform would need to operate on a buyer beware basis. As shared platforms prove themselves and operating models demonstrate the anticipated improvement in regulatory standards and accuracy, it is appropriate to evolve the position on corporate and personal liability. If the shared platform does indeed raise the bar to the point KYC breaches become an exceptional event, there is an argument to shift the focus from penalties and fines to the way in which organisations can optimise operational costs and hence tax revenues resulting from improved financial performance.

That said, it would be a missed opportunity not to consider liability and the art of the possible holistically as part of the overall shared platform philosophy.

Costs and charging

For many of the shared platforms, an appropriate charging model would be relatively straightforward to imagine. However, there are a number of instances where this is not as simple as it may seem. For example, where data from completed activities supports later activities carried out for other participants. In such cases it might be reasonable for larger participants to expect some form of rebate to their charges that reflects the benefit that their activities creates for other participants.

While on the face of it this may appear to be a commercial question, the issue is not straightforward. For example, where there is a plan to mandate the use of such a service, the ability for participants to negotiate on such points is weakened. Additionally, should large incumbents achieve a position where they can influence the tariff for such services there is a risk of the service becoming expensive for new entrant participants and effectively becoming a barrier to entry.

Pricing of these services will need to be addressed early in the creation of the platform. For mandated platforms it would seem reasonable that a tariff should be created in conjunction with government and be published to ensure that pricing is fair and transparent. For shared platform services that are optional, a more commercially led approach should be used although, again, a published tariff book would seem the most effective way of maintaining transparency and fairness. In both cases, implementing a 'pay as you go' model as the basis of the rate card would seem fairest.

ESTABLISHING SHARED PLATFORMS – HOW HARD CAN IT BE?

A number of the shared platforms documented earlier have been discussed in financial services circles for many years. There is general acknowledgement that they could bring significant benefit to the industry, making it more efficient, effective and resilient. However, they all face challenges with either getting off the ground or reaching a meaningful scale of adoption.

We have identified a number of the more substantial constraints that inhibit the ability for such platforms to exist. The following table articulates the complexity of implementing a given shared platform against the amount of support, either in the form of legislative or regulatory changes required to enable their development. It notes the complexity under each field as high and/or medium complexity.

Table 1: Complexity considerations for each of the candidate shared platforms

Source: Deloitte

Shared platform models	Solution considerations/complexity	Regulatory and legal considerations/complexity
Know Your Customer (KYC) Transaction monitoring Fraud prevention	**HIGH** Complex integration landscape – taking information from multiple sources of differing format and quality and standardising this to the extent required to support analysis. Data security on any common, centralised database will be a critical concern. Fraudulent activities cover a broad and growing spectrum. Identification of activities that are potentially fraudulent or suspicious is difficult as it is not easily defined by rules or logic.	**HIGH** Current legislation may actually prevent the sharing of data required to make this solution effective. Regulation will be required to drive full participation in the provision of data – without this there will be an incomplete picture. Where KYC services are provided by a third party rather than each institution there is a fundamental question around what this means in terms of ultimate accountability should issues arise.
Regulatory reporting	**HIGH** If a centralised solution is used for the collation of data and creation of regulatory reports on behalf of institutions this will involve significant integration and data work. If a distributed ledger and blockchain type solution is used this will require the regulator and institutions to adopt new architectures to support this.	**HIGH** Depending on the solution, the regulators may need to fundamentally change the way regulatory requests are communicated and submitted – adopting "smart contracts" for example.
Collateral management	**HIGH** The solution will only be effective with full participation across the industry. There will be complexities with integration to institutions and also to the data validation sources such as Companies House and the Land Registry.	**MEDIUM/HIGH** End to end visibility of collateral will require full participation which will likely require a regulatory mandate. Accountability needs to be explored in terms of using information from the central repository – a bank may still need to use its own data in order to rely on that figure both in terms of Professional Negligence claims on the valuer and for the purposes of Capital Adequacy.
Trade finance	**MEDIUM/HIGH** Potentially complex integration landscape, gathering data or varying formats and quality from multiple sources.	**MEDIUM/HIGH** A complete and accurate understanding of trade finance transactions will require full participation which will likely require a regulatory mandate.
Syndicated loans processing	**MEDIUM** Aggregation of data in a central utility will present an increased data security risk that will need to be mitigated. All transacting parties need to be using the platform.	**MEDIUM** Transfer limitations mean that most of the loans in which institutions participate require the consent from the borrower to allow them to be sold to a third party.

To some extent, the above table is subjective and the authors recognise that there is scope for disagreement on the exact measure of solution and regulatory/legal complexity associated with each platform. Additionally, some new technologies such as blockchain, may mean that technology can solve issues that we currently regard as requiring legal or regulatory change to implement.

Based on analysis of the potential benefits combined with the current appetite in the industry and strategic objectives of government, the concepts of KYC checking (with its parallels to transaction monitoring and fraud prevention) and regulatory reporting were selected for further investigation. The objective of this further work was to look at the practicalities, be they operational, commercial, technical or regulatory, to achieving the desired outcome and the recommendations and actions to be considered by government, regulator and industry to enable that to happen.

Deep dive one – KYC shared platform

At a global level, the scale of money laundering activities is growing, fuelled in part by the increasing access to technology and data that can be used to both facilitate and conceal such activity.

The KYC shared platform concept is based around the creation of a shared platform to support the execution of KYC checks against trusted data, linked unambiguously to an individual or organisation. The hypothesis is that this collective approach to activity monitoring and risk assessment will increase the opportunity to identify suspicious individuals, organisations and behaviours and enable a move to a proactive approach to managing client identity and risk. A shared platform would also support the drive to increase competition in the market by allowing smaller scale organisations to access KYC services on a transactional basis and improve the customer experience through reduced administration and processing time.

There are varying operational models for how such a shared platform might operate. The models that currently exist are based either on a full service capability, where the entirety of the KYC checking and record maintenance is performed on the shared platform, or a high degree of 'trusted' data sharing among participants.

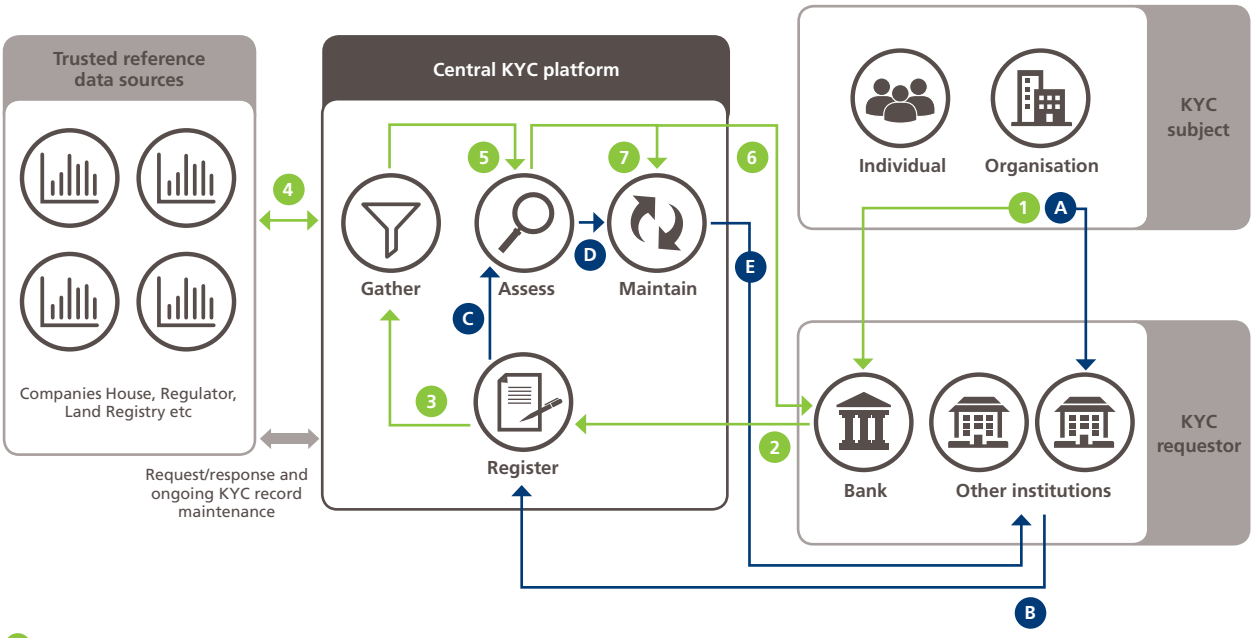
It should be noted that there are other shared infrastructure arrangements that already exist or are being developed in areas such as payments, clearing and settlement and these may provide useful insights as to the operating model that should be adopted for KYC.

Concept operating model

In this section we present a concept operating model for the purposes of drawing out the key operational and technical considerations and challenges associated with a shared platform. It is important to remember that in this context the platform is the technology, process, governance, controls and membership of a shared endeavour. It is just a technology solution or 'rails' the platform could operate on. We intentionally do not advocate one technology solution over another, recognising that there are a range of options, each with their own pros and cons.

Figure 1: Concept operating model for a Know Your Customer (KYC) shared platform

Source: Deloitte



Steps needed for a new or unknown individual or organisation

Steps needed: for an individual or organisation with an existing KYC record

In both of the use cases described above, the responsibility remains with the institution to take the KYC output from the platform and make a risk based judgement, potentially further enriching this with their own data (e.g. blacklist information). The platform is not regulated nor does the platform underwrite the ultimate KYC decision made by the institution. In addition, there will need to be a very clear articulation of the Master Service Agreements and Service Level Agreements with the platform organisation.

It is important to note that there are a range of models that can be used for KYC, not all of which rely on the 'data heavy' centralisation of information described here. Distributed ledger technology and digital identity could be used to provide trusted data and assurance for KYC checks instead. Such a model would leave the execution of KYC checks with individual organisations and opens up the concept of an individual or organisation giving consent for their KYC data to be shared rather than organisations repeating the same checks. The purpose of this paper is not to consider one technical approach over another, and in many cases the underlying challenges to progress, which is the focus here, remain the same.

Operationally, there may be a hybrid model where the platform, to achieve the economies of scale it will require to be successful, will only want to cater for more simple/basic checks. If so, then organisations will need clear decision trees to establish, based on attributes associated with an individual or organisation, whether simple or more extensive checks are required.

Current landscape

KYC platforms have existed in various forms over the last five years. These take the form of client data and document utilities such as KYC as a service, centralised managed service platforms and electronic-ID KYC platforms (such as those in the Nordics and Singapore).

While there has been some success in delivering the benefits the industry was hoping for, existing models have struggled to deliver these at the optimum scale, namely:

- Improved operational efficiency and therefore cost reduction through being able to redeploy operational staff into other duties and focus front office time on selling.
- Improved customer experience (onboarding time/ reduced duplication).
- Improved accuracy and more effective risk management.

The underlying challenges described by those operating KYC platforms that have hampered the success of shared platforms can be categorised as:

- difficulty in reaching consensus on standards
- failure to achieve mass adoption and scale
- absence of the regulatory/industry imperative to drive adoption
- failure to resolve regulatory liability with the liability still sitting with the organisation
- costs have proved to be expensive vs the benefits of using the service
- outdated information as there is no incentive for clients to keep data up to date once provided
- increasing concerns around data privacy/security/sharing
- ensuring that the results of shared KYC outcomes do not inadvertently lock people out of access to financial services.

As discussed earlier in this paper, five of the biggest banks in the Nordics are working together to explore the creation of a joint anti-money laundering solution, which would incorporate KYC. This is scheduled to launch in the latter part of 2018 pending approval from the EU competition authorities. This demonstrates the appetite within the industry to develop solutions that address evolving threats, new requirements and the improved customer experience that comes with improved processing time. In the Nordic model, the solution providing the KYC services will be owned and controlled by the founding banks but will also be able to offer services to third parties.

Key challenges and associated recommendations for KYC

There appears to be a genuine appetite within the industry to actively pursue alternative solutions for KYC and a compelling social and economic need to optimise such processes in order to disrupt and prevent potentially criminal activity.

Work to date across the industry has exposed, or reinforced, a common set of challenges that warrant a broader consideration of how best to enable and support a shared platform from a government and industry perspective.

In order to turn the concept and initial work on shared platforms into an effective and sustainable solution there is a set of clear recommendations that we propose here to address specific challenges. We classify these as high priority if they are essential to a shared platform model operating effectively and lower priority if they enhance or accelerate, but are not essential to, the effectiveness of the solution.

Given the increasing activity in the market regarding KYC and other shared platform arrangements, the authors recommend a dedicated activity across government and industry to identify and review similar projects within the UK and elsewhere. The objective of this work would be to assess the areas of success and failure in order to capitalise on the knowledge that exists and to confirm and begin to address the fundamental barriers to progress.

In addressing these challenges, we recommend drawing upon experience from existing shared infrastructure arrangements in the industry, such as those for payments, clearing and settlement. It is anticipated that this will provide valuable insight with regard to identification, liability and governance – a good example being the work performed to date by the Open Banking Implementation Group in setting up a directory of registration which could have a direct read across into any KYC operating model.

1. Accountability and liability (high priority)

Challenge

One of the thorniest issues facing shared platforms is who bears ultimate responsibility and potentially liability in the event that data which is relied upon turns out to be inaccurate or an assessment fails to identify a fraudulent identity. It is important to clarify at the outset that there is no general legal or regulatory prohibition against outsourcing. Firms are allowed to outsource almost anything to third party providers, with one major exception: as matters stands today, firms are not allowed to outsource their regulatory compliance duties and responsibilities.

A KYC platform model of some description is already possible today, without any change in law or further guidance from the regulators. Firms currently replicate some KYC-related functions across their organisations (e.g. processing and validation of documentation, checking background information, storing information, and so on). While there may be some differences between these functions within firms, there is bound to be a significant degree of overlap and duplication. Assuming a platform could offer these processes and functions in a way that maps sufficiently to firms' existing processes and functions, they should be able to outsource those functions to the platform and then use and quality assure the outcome provided by the utility to complete the KYC process within the firm. Firms would still need to ensure these outsourcing arrangements meet the current legal requirements (including that they retain oversight over the performance of these functions) but this is no different really from firms outsourcing other functions (such as technology and administration services) to third parties.

The challenge, however, is that a firm must retain sufficient oversight over all functions that affect its regulatory status or its regulatory compliance. From a KYC perspective, this means the firm must retain the final decision on whether or not an applicant has passed KYC, based on the firm's own procedures and criteria as well as the outcome of all checks and verifications conducted by the firm. In the full-utility KYC model, the firm would no longer make this decision itself. Instead, the firm would look to the platform to conduct all required checks and processes and – crucially – would rely on the KYC decision reached by the platform for the firm's own KYC purposes. This last aspect in particular (relying on the KYC decision reached by the platform) presents the most fundamental challenge to the adoption of a full-function KYC platform.

What does this mean for the adoption by industry of a KYC platform? In simple terms, while it is currently possible to outsource some KYC-related functions to a platform, as the law stands, firms will not be able to move towards the adoption of a full-function KYC platform without exposing the firm and their senior management to criminal and civil liability.

It is also worth noting another potential regulatory constraint, namely that a platform may present a concentration risk from a regulatory point of view. If a platform becomes a single point of failure risk to the industry, the regulator may in the exercise of its functions encourage or direct firms to explore alternatives. While that is not an immediate concern, it will become more and more of a concern the more successful the platform becomes, and the more firms rely on its KYC functions.

Recommendation: government and the regulator should explore options in conjunction with industry around how the regulatory framework should be adapted for a shared platform model.

The adoption of a full-function KYC platform where the financial services provider no longer has to declare it has verified each KYC check will only be possible if existing regulation is amended. In particular, the risk of firms or their senior management being held liable where they relied on the outcome of a KYC process conducted by a utility, will need to be revisited before outsourcing of KYC functions can move beyond today's limited scope.

Any updated regulatory framework cannot be expected to absolve firms or their senior management entirely, if they choose to outsource. Firms and senior management should be held accountable for a range of matters within their control, backed by civil or even criminal sanction in the event of non-compliance. While these matters will require further consultation, examples could include that firms will be expected to retain responsibility for satisfying themselves with the processes and procedures adopted by the platform as part of the KYC process; for the sources of data and information that the platform will use; and for conducting regular audits and checks on the utility's compliance with its contractual obligations.

Ultimately, the aim will be for firms to be able to rely on the outcome of a KYC process conducted by the platform, without having to conduct any further verifications before arriving at the same conclusion. But even this change could manifest itself in a number of different outcomes, and it is possible that changes could be introduced in stages and over time to move closer to (and eventually create the regulatory environment for) adoption of a full function platform model. As examples:

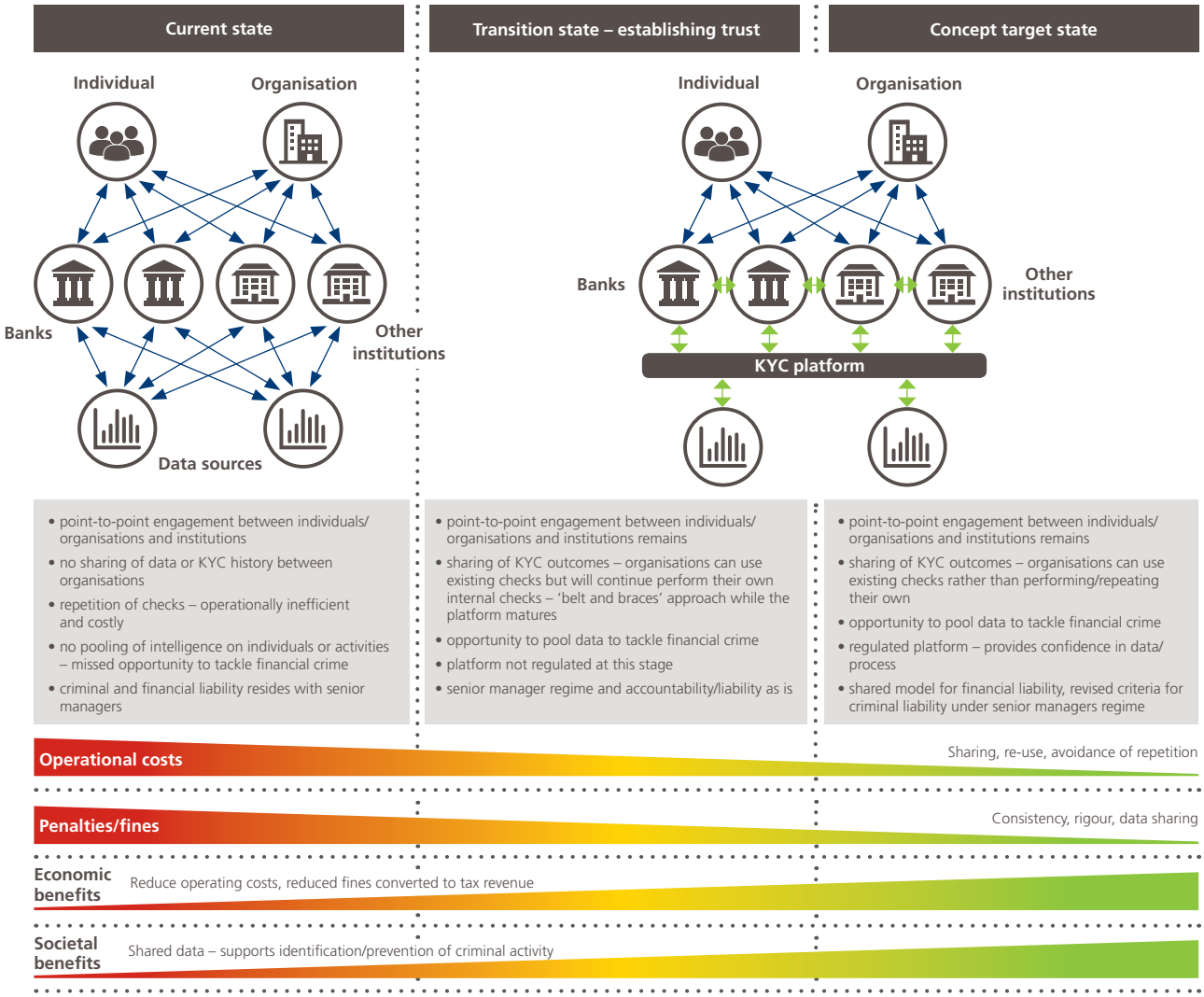
- Option one: the firm and senior management could escape liability (criminally or otherwise) where they are able to demonstrate the platform was contracted to conduct steps and processes that the firm itself would otherwise have taken and that these were adequate for KYC purposes; that the utility followed a decision-making process that the firm would have followed and that these were adequate for KYC purposes; and that the utility came to the same conclusion that the firm would have arrived at. This, though, would still require significant oversight by the firm over the day-to-day activities of the utility, as they would need to demonstrate oversight over the manner in which the utility performed the outsourced functions.
- Option two: as above, but with full day-to-day oversight over the activities of the platform replaced by more infrequent audits and checks.
- Option three: the firm and senior management only have to demonstrate the platform was contracted to conduct steps and processes (including a decision-making process) that the firm would have followed and that these were adequate for KYC purposes – without having to demonstrate that the firm actually complied with these obligations.

In all cases, the senior management would need to be comfortable with how liability/accountability is defined and enforced. Option 3 would get close to the ultimate objective, however given the regulators' current mandate, it is difficult to see why they would accept this without significant discussion and the imposition of additional checks and balances – and potentially even a requirement that the platform should itself become regulated (although outsourcing to a regulated entity does not in itself absolve firms or senior management from their existing oversight responsibilities).

Industry should engage with government and regulators on this. There should be focus in particular on the following questions: if the KYC processes and procedures adopted by the platform would be materially similar to those adopted by the firm, and would have yielded the same outcome, should the platform not be liable in the first (and only) instance? Why should the firm also be liable? In fact, should the firm not be able to claim against the platform?

Figure 2: Illustration of potential transition states to an alternative liability regime

Source: Deloitte



For the utility model to work, the utility would have to have financial exposure to the firms that rely on it for the conduct of the KYC function as an incentive for it to operate correctly and abide by its contractual duties. This, in turn, creates a risk for all firms that rely on the utility, namely that the magnitude of claims could be so significant that the utility could become insolvent or unable to trade. If this were to happen, and if other utilities are not immediately available, firms may be left without the ability to conduct KYC checks (as they would have relinquished their own capabilities to do so). This is an inherent risk in all outsourcings to a common platform provider, and firms will need to engage with their legal counsel and operational experts to ensure adequate exit planning is in place. This may include cooperating with other firms who may be exposed to the same risk.

A number of bodies are currently looking at this challenge, including UK Finance and the TechNation FinTech Delivery Panel. Aligning these studies would help gain consensus and likely yield a quicker outcome.

Until such time as the regulatory model is amended, the ability to outsource KYC-related functions will remain limited, with liability and responsibility remaining with the firm. The benefits of the shared platform will lie in the storage and distribution of trusted data provided to the platform from approved sources and the collation of audit trails of successful KYC activity against the digital identity of an individual or organisation. In reality, the shared platform approach will need to demonstrate that it is increasing standards and operational effectiveness for there to be a compelling driver to consider change in regulation.

Who should lead?

Led by government and the regulator (PRA) in consultation with industry.

2. Clarity of requirement (high priority)

Challenge

The current potential degree of interpretation within regulatory requirements and policies can create an operational overhead in establishing how to execute KYC checks in a reliable and consistent manner. This is a challenge across different regions within countries that only becomes more difficult when you look across jurisdictions.

Recommendation: the shared platform solution should be underpinned by a focus on defining central policies and common standards for data collection and assessment.

Development of a shared platform approach provides the opportunity to develop central policies that delivers data collected and assessed to an agreed standard that is good enough to be used and trusted without additional processing by the banks.

Who should lead?

Joint initiative between regulators (FCA and PRA) and industry.

3. Data sharing (high priority)

Challenge

There are strict rules and protocols governing privacy and banking confidentiality. Depending on the nature of the shared platform approach, it may be necessary to share customer details in addition to transactional information which may require legislation regarding data sharing to be reviewed or, as a minimum, the ability to provide consent to be made as simple as possible.

Recommendation: government regulators and industry should work together on identifying and driving forward the most pragmatic solution to make data sharing as efficient as possible.

In considering the most appropriate long term solution for KYC, which may be different to that used today, the use of data and the ability to link that unequivocally to an individual or organisation is key. In some cases, the effectiveness of the solution may require changes to the associated rules and legislation and the adoption of new technology (e.g. digital identity). Government regulators and industry should work together on identifying and driving forward the most pragmatic solution.

In addition to the sharing/aggregation of data to perform KYC checks, there are also proposed approaches that promote the sharing of KYC outcomes, with the consent of the subject, between organisations. For this to be effective the ease with which consent can be provided should be examined.

Who should lead?

Joint initiative between government, regulators and industry.

4. Trusted sources of data (high priority)

Challenge

There is an increasing challenge to the validity of the current trusted sources of data (e.g. data from Companies House) as a result of time delays in updating that data and questions over governance. This results in organisations reverting to their own source data which in turn removes independence.

Recommendation: agreement needs to be reached between regulators at a regional, and ultimately, a global level on data standards and the provenance of data into and out of the shared platform.

Government will continue to have a pivotal role to play as a 'gold standard' data provider, applying trusted data standards and processes across different departments (HMRC, Treasury and DCMS).

Who should lead?

Joint initiative between government and industry.

5. Identity and security (high priority)

Challenge

The creation of an indisputable identity for the individual or organisation subject to the KYC check to ensure the accuracy and provenance of the KYC information.

Recommendation: government should consider the drive towards digital identification at scale as a strategic objective.

A number of pilot projects are underway around the concept of a Digital ID and it is often developing countries that are paving the way. That breadth of adoption in turn drives the rapid development of new services underpinned by the Digital ID.

In India for example, the implementation of centralised or shared platforms has been helped by the widespread adoption of a national identity scheme. In addition, use of Digital ID has become ingrained in normal life as the mechanism to engage public and private services in an efficient way. While the UK has experienced challenges in the past with the implementation and adoption of identity schemes such as ID cards, the landscape has changed significantly in recent years. Observations from other countries suggest that the population is now more aware and accepting of the need for, and benefits of using, a unique and verifiable identity. The hypothesis is therefore that in this day and age, a Digital ID will be recognised as an enabler for ease of access to a range of public and private services and not simply as a potentially unwelcome extension of state supervision and control. On that basis, government should consider the drive towards digital identification at scale as a strategic objective.

For institutions, there is the concept of a business passport, detailing the known and trusted details of an organisation. Identity is a more difficult concept to manage for an organisation. Typically, identity has been derived from records such as those held by Companies House or the Land Registry, however this is not appropriate for all organisations. One emerging concept is to examine banking transaction data and behaviour as an additional way of assuring the authenticity of an organisation. Other techniques look for patterns in data, for example where organisations are operating fraudulently, perhaps by closing and then creating new businesses or opening multiple businesses in parallel. There are analytical techniques that can be used to spot trends in common data points between apparently unrelated companies that can indicate suspicious behaviour.

Who should lead?

Joint initiative between government and industry.

6. Market participation (high priority)

Challenge

A full scale, operational solution ultimately requires broad market participation to be truly effective. As it stands, there is no common technical standard or architecture to govern the way in which institutions would engage with a shared platform. It is also not clear how an institution would best identity the point at which a tipping point had been reached where it became sensible to move KYC activities at scale to a new shared platform.

Recommendation: starting at the regional utility level, regulators in collaboration with industry, should work to define a set of common standards (technical, data and process).

While open architectures and common interface standards are increasing, significant issues exist with interoperability and the prevalence of different standards and protocols.

Starting at the regional utility level, regulators in collaboration with industry should work to define a set of common standards (technical, data and process) through a series of joint working groups and pilot initiatives. By starting at a regional level and expanding from there may also allow a gradual versus big bang adoption of any new platform. Adoption may in turn drive opportunities for organisations to realise a revenue stream from establishing and running shared platform services to common, accepted standards.

Voluntary adoption of the shared platform approach may not be effective on its own. By working to clear the technical and operational barriers that exist and through demonstrating the associated benefits, such as reduced operational overheads, the respective regulators will then be in a position to credibly mandate participation in a shared platform solution should that be required.

Who should lead?

Joint initiative between government, regulators and industry.

7. Ownership, operational and commercial models (higher priority)

Challenge

The creation and ongoing operation of a shared service platform is a significant undertaking. One of the fundamental questions to be addressed is who will own, manage and fund the shared platform.

There are a number of operational and commercial models which could be explored, and the pros and cons of each vary:

- Government owned and operated – how would this be funded and what does this mean for liability and responsibility?
- Consortium model (all private or public/private) – in addition to the liability model what is the commercial construct in terms of investment and return. Should this be not for profit for example?
- Institutional ownership – it is possible that a large bank could own and run a platform in a region, but is this feasible on a larger scale and what does this mean for independence?

Within this decision there sits a range of broader topics around governance and control, how membership is agreed and managed and how disputes are resolved to name but a few. Additionally it would be need to be agreed how the platform is to be capitalised, both during the initial set-up period and in the longer term, where the platform may be running as a separate regulated entity.

As it stands, the balance of opinion looks to favour a public/private joint approach that blends the critical ownership and leadership from industry with the regulatory permission and security of a significant regulatory involvement.

Recommendation: establish a working group to look at the ownership, target operating and commercial models. Current activity in the market, as described in the current landscape section above, shows that some form of consortium approach, either between banks or involving a third party, has some momentum already.

Establish a working group to look at the target operating model and consider whether government action or endorsement is required. The early view is that a consortium model may be favoured, with the government inviting a cohort of participants to sign up to pilot a platform.

From a commercial perspective, a potential cost share model could be used where the central platform bears the initial cost of performing the KYC check but the parties that subsequently consume that KYC output contribute, for example, 20% of the cost to use the KYC outcome.

That could mean a relatively rapid payback period for performing the check and a reduction of 80% in each cost per check.

Who should lead?

Joint approach between government, the regulators and industry.

8. Regulatory alignment (lower priority)

Challenge

Global standards and regulatory requirements are, if anything, diverging rather than converging due to differences across geographies and jurisdictions as well as the way in which global banking is evolving.

For example, organisations with a large US presence or those headquartered there may only be willing to devote the resources necessary if it was clear the platform would not be run simply in parallel to US systems.

Recommendation: government should promote UK prototypes/experiences in global fora and in the FCA's Global Financial Innovation Network to move the wider industry towards regulatory alignment wherever practical.

Government will be best placed to drive the discussion on how alignment across jurisdictions will operate to avoid regulatory isolationism impacting the effectiveness of the shared platform. This is a very different model to the clear line of accountability that exists today and the behaviours this would drive and protections this would provide need to be explored.

While the ultimate end goal is a global set of common standards, the recommendation is to progress in a two phased approach.

- Develop regional platforms where regulatory requirements are consistent and where common technologies are more likely to exist. Tight collaboration between regulators and trusted data providers in the region will be essential. In this model it is also feasible that a large financial institution in the region may take on the running of the shared platform.
- Once a network of regional platform exists and there is a wealth of experience of regulatory, technology and operational considerations, then look to move to combined regional and ultimately a single global solution.

Addressing the requirements of the US regulator will be key in developing any truly scalable global solution. A sensible aim should be a longer term merging of initiatives with the US and other significant financial services markets. That said, as the leading global hub a UK system/platform would by default have international appeal so there is still the opportunity for progress to be made as alignment develops.

The FCA's global sandbox initiative should be a key asset in helping navigate these challenges and we recommend that KYC be made a subject for discussion through the Global Financial Innovation Network.

Who should lead?

Government and the regulator (FCA), in conjunction with industry.

Deep dive two – regulatory reporting

Both the Bank of England and the FCA have demonstrated a commitment to exploring ways to improve the efficiency of end to end regulatory reporting processes. Their mission and goal in this space is frictionless regulation through delivering machine readable and executable regulation.

Currently, regulatory requirements are open to a degree of interpretation by institutions. At best, this results in a significant number of institutions trying to codify the exact same rules and programmes to generate the correct reporting and metric outputs required by the regulator. At worst, this significant effort can still result in inconsistent responses back to the regulator due to differing interpretations of the ask – resulting in time consuming analysis and follow up requests.

Whatever the outcome, the current approach also results in significant volumes of data transmission and duplication between the institutions and the regulators without necessarily supporting any form of secondary data analysis or the ability to react to incremental data changes. Instead the process drives periodic, large volume data transmissions with potential inconsistency and ambiguity in content.

For the purposes of this paper, we consider the concept operating model associated with a distributed ledger based solution. A distributed ledger (or shared ledger) is a type of database or application that is replicated, shared, and synchronised across multiple sites, countries or institutions.

The rationale for focusing on this approach is that it is currently in pilot, has some tangible lessons learned and known challenges. It is viewed as the most likely approach to succeed as it retains the direct input and accountability of the submitting institutions rather than devolving this to an, as yet not existent, common reporting function. The key benefits anticipated with this particular approach are:

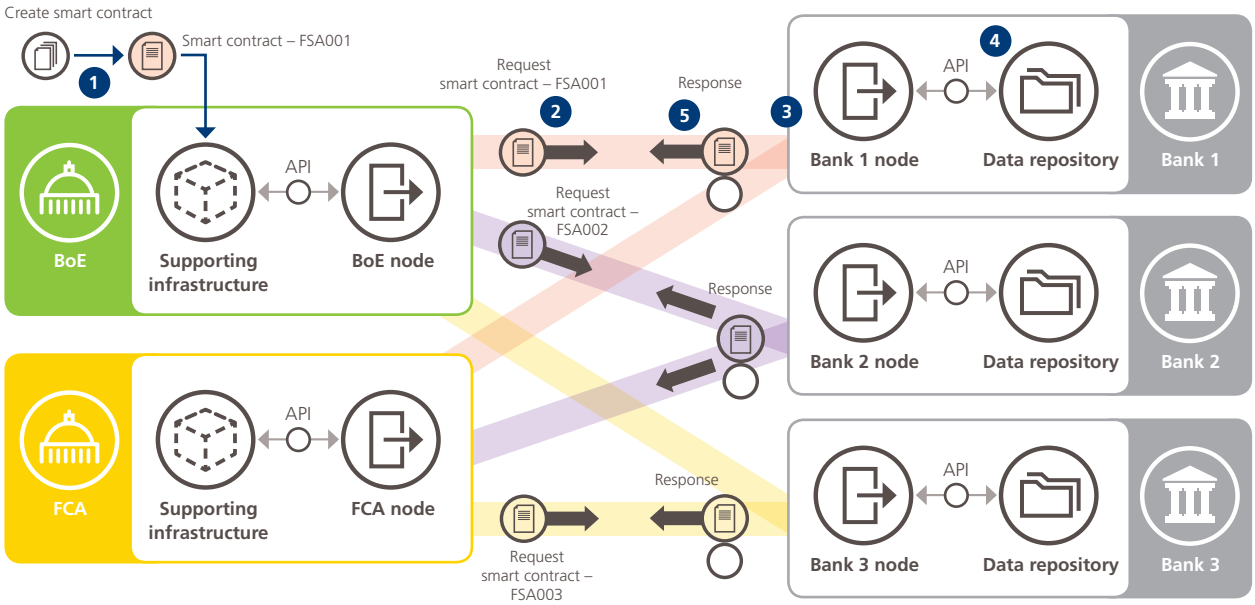
- Interpreting the regulatory handbook into smart contracts improves efficiency, consistency and flexibility.
- Improved data security – the data remains within the financial institution rather than there being large data transmission to the regulator.
- More granular data is available through the use of common data models.
- There is ad hoc availability for regulators rather than the more limiting periodic data submission schedule.
- A distributed infrastructure solution can reduce costs by distributing the burden of computing power and removing duplication of data storage.
- Driving organisations to improve their data quality and standardisation.
- Supports delivery of the key themes around making it easier to do business, driving efficiency, improving profitability etc.

Concept operating model

The concept operating model described below mirrors the current proof of concept being developed for the Bank of England and FCA. While the ultimate operational solution may see some differences, the fundamental principles of operation are likely to be similar to what is discussed here.

Figure 3: Concept operating model based on the current proof of concept being developed by Santander, Bank of England (BoE) and the Financial Conduct Authority (FCA)

Source: Deloitte



The concept operating model currently being developed would operate as follows:

- The regulator defines the specific regulatory ask, be that data or metrics, through the definition of a 'smart contract' – this is a structured, machine readable request that the receiving party can execute against their data. The Regulator uploads this smart contract to its 'node'.
- Distributed ledger technology is then used to circulate the smart contract and to request institutions to accept this. Each institution operates its own secure node on the distributed ledger. This means that while the smart contract request will be common across institutions, each response to the regulators is private and not shared between institutions.
- The institution then accepts or rejects the installation of the smart contract, based on a defined approval process. If accepted, the smart contract code is installed on the institutions 'node' on the network.
- The regulator can then request the smart contract programme to be executed in the specific institution (e.g. Bank 1) via a request to the corresponding node. The programme is then executed in the Bank 1 node using Bank 1 data.
- The output is then made available to the Bank of England and FCA who receive the results across the network at their node along with a cryptographic key that is created as part of verifying the authenticity of the submission.
- Should the regulators require any additional data, they can request this via an API interface using the associated cryptographic key.

The solution that is currently being trialled uses open source ledger technology and common APIs, the objective being to maximise the ease of adoption of the solution across institutions.

Current landscape

In order to create and develop ideas to achieve this 'frictionless regulation', the Bank of England and FCA organised a techsprint in November 2016 and invited firms and universities to attend. The purpose of the sprint was to prove the feasibility of a shared unambiguous data set and create machine readable rules. The team from Santander created the idea called 'SmartReg' to help address the inefficiencies in the process through the creation of a system to execute and evidence machine readable rules. During Q1 2017, regulators asked for the idea to be explored further and a small project was launched in June 2017 which is ongoing.

The aims of the proof of concept are:

- To test the application of distributed ledger technology.
- To provide a consistent digital interpretation of the FCA handbook by codifying this into 'smart contracts'.
- To promote frictionless, machine readable and executable regulation – removing the current opportunity for interpretation of the FCA handbook and the associated ambiguity this can cause.
- Intelligent search and assistance informed by the content of the submissions – allowing more specific, tailored regulatory asks.
- A mechanism to progress to a shared taxonomy, data model and standards – which in turn drives ease of adoption.
- Simplification of the architecture for the FCA and the firms.
- Creation of a potential framework for self-regulation – moving from a 'push' model to a 'pull' model.

Key challenges and associated recommendations for regulatory reporting

The concept of 'frictionless regulation', particularly in an environment where regulatory asks are increasing and the use and interpretation of data is increasingly complex, is very much welcomed by the industry and regulator alike.

To date, the proof of concept has exposed a number of challenges and opportunities in the creation of a common regulatory reporting platform and we believe there is a set of clear recommendations for consideration by government and industry. We classify these as 'high priority' if they are essential to a shared platform model operating effectively and 'lower priority' if they enhance or accelerate, but are not essential to, the effectiveness of the solution.

1. Clarity of requirement (high priority)

Challenge

Regulatory transparency is set as a goal for a shared platform solution and is core to the technology solutions that are being trialled. To achieve this, regulators need to adopt new ways of working and to encapsulate regulatory requirements in smart contracts.

By increasing the precision of a regulatory requirement and removing the element of interpretation the outcome will be that 'you get what you ask for' and no more or less. While this improves consistency, the information may lose a degree of richness that comes with the current variation in interpretation of regulatory requirements across a range of institutions which better inform broader asks.

Regulatory convergence across regulators and across geographies/jurisdictions is a significant advantage and should be considered a key enabler as it makes it easier to define a common set of regulatory asks.

Recommendations:

1. **Regulators need to define their data requirements more clearly and co-ordinate their data requirements with each other. Regulators should take the lead on developing new solutions and approaches to enable the definition and communication of regulatory requirements in a way that removes interpretation and scope for ambiguity.**
2. **The industry will need to address the common challenges around data quality and consistency of standards within and between organisations.**

The regulator should adopt new technologies and processes, such as the adoption of smart contracts, for the definition and communication of regulatory requirements as this removes interpretation and scope for ambiguity. A more purpose based, outcome focused approach to the definition of regulatory requirements will need to come with the acceptance that there will be a period of learning as this model establishes itself.

The industry will also need to address the common challenges around data quality and consistency of standards within and between organisations as this new approach to reporting will quickly expose shortcomings in data.

Who should lead?

1. Led by the regulators (FCA and PRA) in consultation with industry.
2. Industry

2. Accountability and liability (high priority)

Challenge

The challenges from a legal and regulatory perspective are less acute than those described in respect of the KYC platform model.

In the regulatory reporting space, while firms already outsource a fair amount of the work in relation to the preparation of regulatory reports to third parties, they remain responsible for validating that those reports are accurate, complete and submitted in accordance with applicable requirements (including as to timing) imposed on the firm.

Recommendation: government and the regulator should explore options in conjunction with industry around how the regulatory framework should be adapted for a shared platform model.

There is an additional challenge with the regulatory risk reporting shared platform, and that is that firms' requirements can be vastly different, so the level of centralisation that is ultimately possible could be less than in some other utility models.

The question of how liability may differ in a shared platform model is consequential of the regulator needing to be precise in their specification of the smart contract and what happens in the event that an organisation accepts a smart contract but the underlying data which populates the response or the interpretation of that data is misleading.

Who should lead?

Led by the regulator (Bank of England) in consultation with industry.

3. Collaboration (lower priority)

Challenge

The overall success of the solution and realisation of the collective benefit requires collaboration in a competitive market – even if regulatory compliance is not a traditional competitive topic.

Recommendation: a culture change, led from the top, is required to promote collaborative ways of working.

There will be a culture change required to move to a more collaborative way of working – between institutions and the regulator. The ability to define smart contracts that yield the right results and provide the level of data quality required to service them will take time to mature and will require collaboration and patience.

The ability to clarify the ultimate benefits case and to get industry wide recognition for, and buy-in to, this will be key.

Who should lead?

The regulator (Bank of England) in consultation with industry.

4. Lack of precedent (lower priority)

Challenge

A shared regulatory reporting platform is something for which there are currently very few or no precedents set – particularly with the goal of creating a solution using open source and vendor agnostic technology.

Recommendation: continue with the proof of concept approach, while also considering how to then move quickly to scale into production.

The principles of adopting open source, vendor agnostic technologies are sensible in terms of keeping costs low and driving ease of adoption.

The proof of concept approach is working and driving innovative thinking – this should continue and, at an appropriate time, be scaled to provide further insight around what a full scale solution might look like.

Who should lead?

Joint activity between the regulator and industry – using initiatives such as sandboxes.

5. Commercial models (lower priority)

Challenge

The commercial model for establishing the solution and then running it as a going concern could take various forms. Should this be government owned and funded or could/should it be run by industry or the wider private sector? There is a strong case to be made that where the benefits will be realised by the private sector, then the cost should be borne by industry.

Recommendation: establish a working group to look at the target operating and commercial models.

Establish a working group to look at the target operating model and the pros and cons of the varying ownership model: As discussed above, these include:

- Government owned and operated – how would this be funded and what does this mean for liability and responsibility?
- Consortium model (all private or public/private) – in addition to the liability model what is the commercial construct in terms of investment and return. Should this be not for profit for example?
- Institutional ownership – it's possible that a large bank could own and run a platform in a region, but is this feasible on a larger scale? And what does this mean for independence?

Who should lead?

Joint approach between government, the regulators and industry.

6. Appetite for change (lower priority)

Challenge

Sponsorship and conviction from all interested parties will be needed to deliver what is a fundamental operational change.

Recommendation: articulate a clear benefits case and broader incentives for adopting a shared platform solution.

In an ideal case the concept of frictionless regulation will be enough to drive the high level of adoption needed to make the solution viable.

In some cases, the pace of adoption of any change may not be sufficient and a clear regulatory incentive and benefits case will need to be articulated for participants. Ultimately, if this is insufficient then mandated adoption may need to be considered.

Who should lead?

Joint approach between government, the regulators and industry.

CONCLUSION

As noted at the outset of this document, the shared platforms advocated have the potential to ensure the UK retains its reputation as a global leader in FinTech innovation, particularly within the regulatory space. The successful development of any of the seven platforms mentioned above would create a highly in-demand export which would bolster the UK economy.

The recommendations on liability, regulatory alignment and data sharing are fundamentally about updating the current frameworks for the digital age. We have in each case sought to strike a balance which is fair and which recognises that traditional business models are changing.

More broadly, the collaborative approach embodied in the platforms will benefit consumers by both enhancing transparency and driving competition. On the first, the shared platform will often enable regulators to analyse to a much greater depth the transactions being conducted across the wide range of subscribed firms and identify potential risks at an earlier stage, protecting consumers from cybercrime and fraud. With the second, the cost efficiencies for firms will both assist new entrants to the financial services sector, and enable consumers to much more easily switch their bank account, bundle their pension pots, and apply for new financial products.

Technology has driven the core of financial services for many years. We believe the UK is ideally placed to leverage our position and understanding of financial markets to drive innovation in the market for years to come. Shared platforms offer one such avenue for the UK to pursue.

A final note on appetite

Established providers

In many cases the implementation of a shared platform may not have a direct financial benefit for incumbents. In the worst case, there may even be a potential additional cost. There is also a case to argue that the creation of such shared platforms can make it easier for new entrants to enter the market and that these solutions therefore actually increase the competition facing established providers. However, throughout the creation of this document representatives of industry incumbents that were canvassed typically indicated strong support for shared platforms where they improve our industry's ability to fight crime, reduce risk or create potential efficiencies.

Policymakers and regulators

In any case where there is a requirement for regulatory or legal change there must, by definition, be support from the regulators or legislation to make that change possible. In some cases, such as fraud and transaction monitoring, there is a very strong case for a coordinated global approach to resolving these barriers. However, the creation of shared platforms could be perceived to be allowing incumbents to unburden themselves of certain responsibilities, for example through handing off fraud tracking to a third party. While this is a valid concern, the upside of the creation of coordinated and centralised functions for these activities must surely outweigh any concerns about being able to hold incumbent senior managers responsible for failures in these areas.

For further information about this report contact:

Louise Brett, Partner and FinTech leader, Deloitte North West Europe
lbrett@deloitte.co.uk
+44 (0)20 7303 7225

Brian Fulthorpe, Partner, Deloitte
bfulthorpe@deloitte.co.uk
+44 (0)20 113 292 1625

Marcus Scott, FCA, Chief Operating Officer, TheCityUK
marcus.scott@thecityuk.com
+44 (0)20 3696 0133

Marcus Corry, Policy Manager, TheCityUK
marcus.corry@thecityuk.com
+44 (0)20 3696 0108

TheCityUK

TheCityUK, Salisbury House, Finsbury Circus, London EC2M 5QQ
www.thecityuk.com