



NEW TECHNOLOGIES AND ANTI-MONEY LAUNDERING COMPLIANCE

FINANCIAL CONDUCT AUTHORITY

31/03/2017



EXECUTIVE SUMMARY



Richard Grint

Financial Crime Consulting Lead, PA Consulting Group



Chris O'Driscoll

FinTech and Risk Analytics Lead, PA Consulting Group



Scott Paton

Senior Partner and Head of Risk & Compliance, PA Consulting Group

This report details the findings from a study into new technologies in Anti-Money Laundering (AML) compliance by PA Consulting Group (PA) on behalf of the Financial Conduct Authority in the UK (FCA). This report represents the culmination of three months of research and over 40 interviews with regulated firms, technology providers, and other bodies.

The purpose of this report is to provide clear answers to a number of key questions set by the FCA, namely:

- What new and emerging technologies are available with potential applications in AML? Of these technologies, which are the most promising and which are being considered by regulated firms?
- What are the views from the technology providers around innovation in AML compliance, including the key challenges they are facing?
- What are the views on the FCA's approach to new technologies in AML compliance?

Many new technologies were perceived as having potential in AML compliance, with

regulated firms slowly trialling a wide variety of innovative solutions both to manage their financial crime risk and to reduce operational overheads.

- For onboarding and maintenance, many firms had considered or trialled new technologies, with utility technologies perceived as the most popular.
- For client screening, firms were particularly focussed on using analytics techniques and machine learning to increase the accuracy of their screening rates to diminish the impact of false positives.
- Transaction monitoring was the area where new technologies were broadly considered to have the most potential – particularly in using data analytics, machine learning and natural language processing (NLP) to enable firms to spot suspicious transactions and assess their risk in real time.
- New technologies were also considered to have the potential to make a positive impact on reporting and management information (MI) – particularly through the use of data visualisation techniques to allow firms to gain insights into their customer base and better manage their AML operations.

Of the various technologies considered during this review across the AML lifecycle, the most highly regarded by respondents were those related to data analytics, machine learning and NLP all of which were considered to have potential for transforming almost every part of the AML compliance lifecycle.

Respondents from the technology sector were cautiously optimistic around the marketplace for their technologies and services. Many felt that they had technologies that were proven, robust and able to significantly improve the way in which regulated firms approach AML compliance. However, they face a range of obstacles to wider adoption, including some scepticism about their capabilities from larger Financial Services firms.

Views on the FCA were generally positive, with respondents citing recent innovation initiatives such as the Sandbox as particularly welcome. However, they also highlighted a number of areas where they would prefer to see greater action taken by the regulator, including updating regulations/guidance to reflect the emergence of new technologies (including the broad adoption of digital channels), as well as potentially facilitating further industry-wide discussions on AML compliance and relevant new technologies. Many of these issues, particularly around new regulations or guidance, are not specific to the FCA but reflective of a global trend whereby lawmakers and regulators struggle to keep pace with new technologies.

In summary, it is clear that new and emerging technologies have genuine potential to have a transformative impact on AML compliance, both in helping to prevent money laundering and in reducing the cost of compliance. However, it is equally clear that substantial barriers to widespread adoption exist, which may well continue to limit the progress of ongoing innovation in AML compliance.

CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION NEW TECHNOLOGIES AND ANTI-MONEY LAUNDERING COMPLIANCE	4
Background to the review	5
Scope of the review	6
Review approach	7
A SHIFTING LANDSCAPE TECHNOLOGY IN ANTI-MONEY LAUNDERING COMPLIANCE	9
Background to the topic	10
Focus of the section	10
Overall conclusions	10
AML technology decision making considerations	11
Customer onboarding and maintenance	13
New technology spotlight	18
Client screening	19
New technology spotlight	22
Transaction monitoring and filtering	23
New technology spotlight	26
Reporting and management information (MI)	28
New technology spotlight	31
BREAKING DOWN BARRIERS THE VIEW FROM TECHNOLOGY PROVIDERS	32
Background to the topic	33
Focus of the section	33
Overall conclusions	33
Barriers facing AML / KYC technology firms	34
Wider industry challenges facing AML technology firms	36
Collaboration across entities	37
‘A GOOD START, BUT MORE TO DO’ INDUSTRY VIEWS ON THE FCA’S APPROACH TO NEW TECHNOLOGIES IN AML COMPLIANCE	38
Background to the topic	39
Focus of the section	39
Overall conclusions	39
Steps FCA could take to further innovation within AML	40
Differences between UK and other jurisdictions’ approach to AML / KYC innovation	43
APPENDIX 1: LIST OF INTERVIEWED PARTIES	44
APPENDIX 2: LIST OF KEY FOCUS AREAS	47
APPENDIX 3: GLOSSARY	50
APPENDIX 4: SUMMARY TABLE OF TECHNOLOGIES	53

INTRODUCTION

NEW TECHNOLOGIES AND ANTI-MONEY LAUNDERING COMPLIANCE



Background to the review

The worldwide AML compliance landscape has changed enormously over the past twenty years, with increasing layers of regulation added in many jurisdictions to strengthen the financial system against money laundering, terrorist financing and other financial crimes. Regulations and regulatory enforcement have continued to become more stringent in recent years, with substantial fines being levied where breaches have been identified.

In response to this continuing regulatory change, regulated firms have built substantial operations to enable compliance and mitigate the risk of financial crime. These activities have consisted of changes to processes, new supporting IT systems and the development of entirely new operational areas. Collectively, this has resulted in a considerable overhead for regulated institutions.

The past twenty years have also seen an enormous amount of technological change.

This has accelerated in recent years with the growth of the compliance technology sector in many mature Financial Services markets. These disruptive and additive technologies were widely considered by respondents to have enormous potential in transforming Financial Services, with many having prominent use cases impacting financial crime compliance, particularly AML.

In light of these regulatory and technological shifts, the FCA commissioned PA Consulting to undertake a study of the new and emerging technologies impacting AML compliance, to better understand which are being considered by regulated firms and which are considered to have future potential. In addition, the study also collected views on the FCA, including perceptions about their approach to innovation and activities that respondents would like the FCA to undertake in the future.

Scope of the review

The scope of the review was designed to look at the key areas relating to new technologies in AML, as aligned to the exam questions of this study:

- What are the key functions of new and emerging technologies related to AML compliance, and how might they aid compliance activities?
- What challenges might firms face in introducing new technologies?
- What good practice examples and lessons learned are available for firms considering new compliance technologies?
- What steps could the FCA take to encourage more innovation in this space?

In order to answer these key questions, a number of key focus areas were identified for investigation. A full list of these is included in Appendix 2 of this document.

The new technologies considered were:

- Those aimed at streamlining or automating Customer Due Diligence (CDD) checks (e.g. video KYC, device-led checks)

- Those aimed at strengthening anti-impersonation checks (e.g. biometric technology, use of third-party ID mechanisms)
- Those supporting the sharing of CDD data between institutions (e.g. third-party industry utilities)
- Those aimed at monitoring transactions for suspicious activities (e.g. machine learning/analytics activity)
- Any other technologies aimed at helping firms comply with the Money Laundering Regulations 2007.

The review was conducted over a three month period in early 2017 and reflects a point in time view of the AML technology landscape, which will continue to evolve on an ongoing basis.

The findings reflected in this report are the result of an extensive series of interviews across regulated firms, technology firms and other bodies, along with the expert input of the PA resources leading the study.

Review approach

Our approach to undertaking this review consisted of three key elements:

Interviews with selected parties

We undertook 42 interviews across regulated firms, technology firms and other bodies.

Within each of these groups, care was taken to achieve a representative balance of respondents. For the regulated firms, we interviewed a variety of different sized retail banks, investment banks, insurers and asset managers. Similarly, for the technology firms we interviewed a targeted shortlist of firms of different sizes which used a range of different technologies.

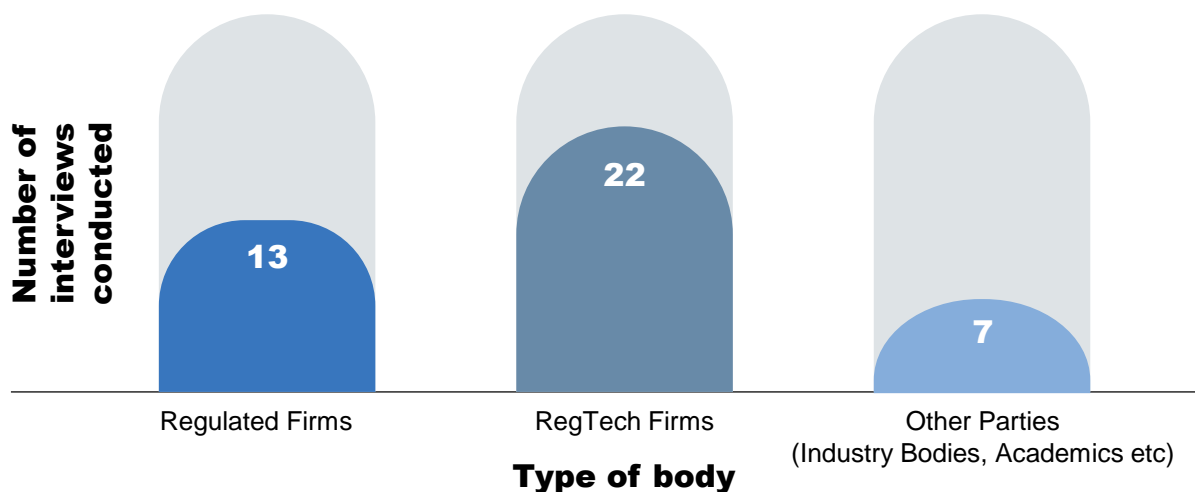
Each interview was undertaken using a questionnaire aligned to the key focus areas for the study. These interviews were conducted by Financial Crime and technology SMEs from PA Consulting and the FCA presence at these meetings was limited by agreement to ensure we received impartial views from respondents. No FCA staff were present for any interaction with regulated firms.

Desk-based research

To complement the perspectives shared in the interviews, we also undertook desk-based research aligned to the agreed key focus areas. This desk-based research consisted of two key elements:

- Exploration of which new and emerging technologies could support aspects of financial crime compliance.
- Analysis of media and academic viewpoints to determine which technologies were perceived as most promising, particularly in an AML context.

The findings from the desk-based research were also tested in the various interviews, where relevant.



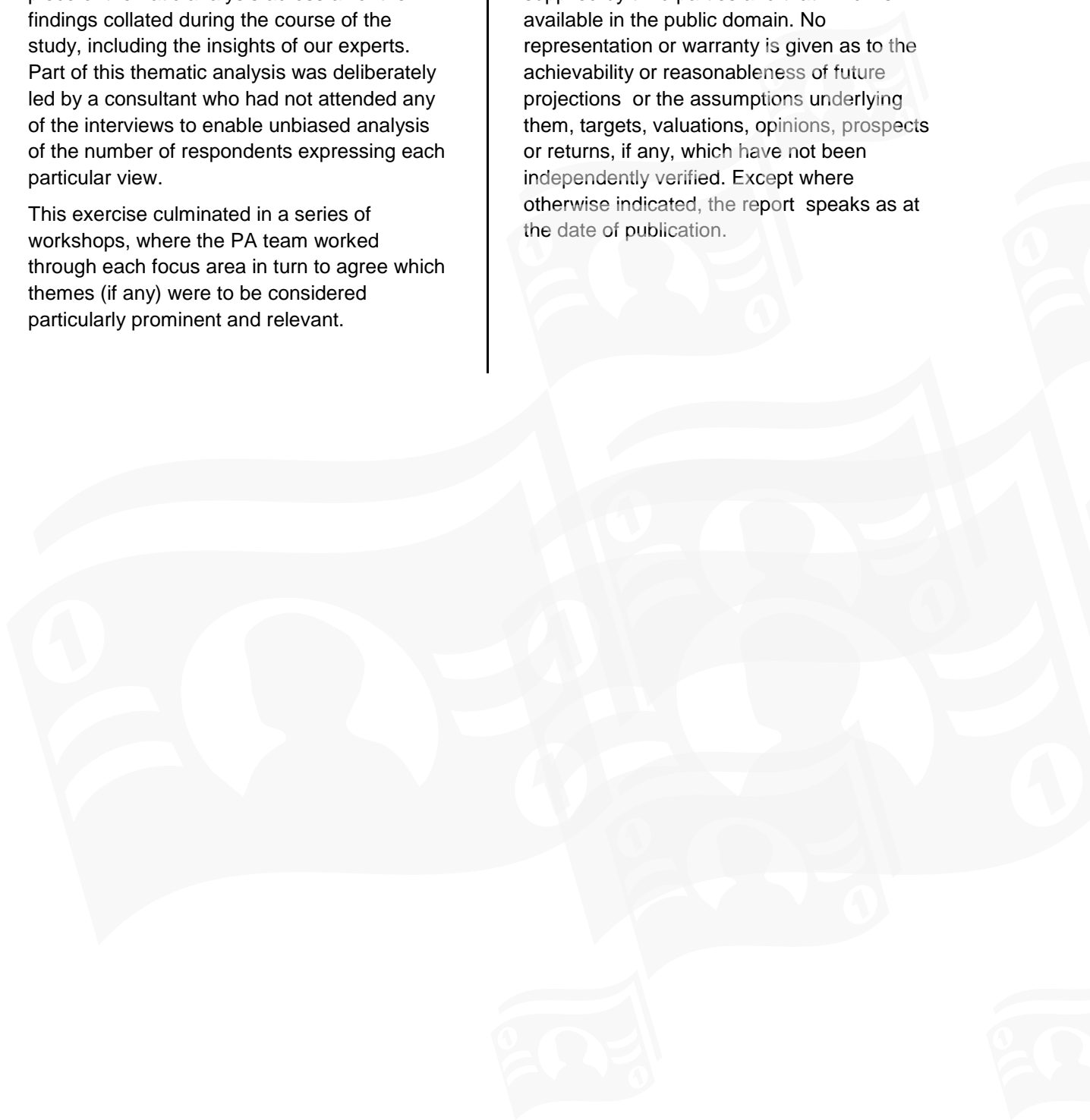
Thematic analysis

Once both the interviews and desk-based research were completed, we undertook a piece of thematic analysis across all of the findings collated during the course of the study, including the insights of our experts. Part of this thematic analysis was deliberately led by a consultant who had not attended any of the interviews to enable unbiased analysis of the number of respondents expressing each particular view.

This exercise culminated in a series of workshops, where the PA team worked through each focus area in turn to agree which themes (if any) were to be considered particularly prominent and relevant.

Disclaimer

This report has been prepared by PA Consulting Group on the basis of information supplied by third parties and that which is available in the public domain. No representation or warranty is given as to the achievability or reasonableness of future projections or the assumptions underlying them, targets, valuations, opinions, prospects or returns, if any, which have not been independently verified. Except where otherwise indicated, the report speaks as at the date of publication.



A SHIFTING LANDSCAPE TECHNOLOGY IN ANTI-MONEY LAUNDERING COMPLIANCE



Background to the topic

The pace of technological change has continued to advance significantly over recent years, bringing with it a host of new technologies with promise for AML compliance. This includes industry utilities, biometrics/video KYC, data analytics, machine learning, NLP and blockchain/distributed ledger technology. All of these technologies have significant disruptive or additive potential, with many having the potential to dramatically increase the efficiency of regulated firms' activities to tackle financial crime.

However, adoption of many of these technologies has been slower than some anticipated, with several firms suggesting that legislation and regulation have been unable to keep pace with technological change.

Focus of the section

This section focusses on a number of key areas of the AML lifecycle and the potential technologies within those areas: customer onboarding and maintenance, customer screening, transaction monitoring/filtering and MI/reporting, as well as detailing any overarching trends in the technology landscape.

In addition, the section contains a number of examples of specific technologies that were prominent in the study.

Overall conclusions

Overall, there were a substantial number of findings from the study of this complex area, with a number of key emerging themes. Some of the more prominent ones included:

- New and emerging technologies have the potential to deliver both significant cost reductions in operational areas as well as significant enhancement of money laundering/terrorist financing/fraud prevention.
- Adoption of these new technologies generally remains slow, with economic, regulatory and operational challenges cited as the reason. Many of these are unique to individual technologies, but with common concerns such as data privacy and data quality regularly identified.
- Some technologies have stronger support than others. Respondents were almost universally excited by machine learning and NLP, but divided on blockchain-based approaches.
- Many of the most promising use cases of technology depend on collaboration between regulated firms, such as agreeing standardised approaches to transaction monitoring. The overarching view is that this is unlikely to happen in the short to medium term without regulator intervention.

The attractiveness of these technologies can vary significantly from institution to institution, with larger firms generally considering themselves better placed to benefit from efficiencies.

AML technology decision making considerations

One of the key focus areas for this study was the priority requirements for regulated institutions when deciding which solutions to implement. During the course of the study it became clear that firms are taking diverse approaches, both in terms of the areas of the AML lifecycle they are focusing on, and the technologies they are using.

In particular, the overwhelming message from the regulated firms was one of risk aversion – many expressed a clear preference for proven capability wherever possible. This related to both providers and the underlying technology itself, with many regulated institutions saying that they felt that the risk of using unproven technologies was too high.

Multiple regulated firms said that making the decision to employ any new technology in AML was a leap of faith, with many suggesting that the size and scale of recent fines in this area have created a culture where any risk of failure or noncompliance is considered to be unacceptable.

Many institutions also noted that cost was often a key consideration. A new technology was significantly more likely to be adopted if it could provide financial as well as compliance benefits.

Regulated institutions also felt that there were a number of issues internally that were a key consideration in determining whether to use new technologies. Notably, many felt unable to move ahead with more complex emerging technologies such as blockchain or machine learning due to a perceived lack of internal technology capabilities. There was a consistent view that without being able to truly understand and operate these technologies themselves, firms would have difficulty convincing the FCA and other regulators of their suitability.

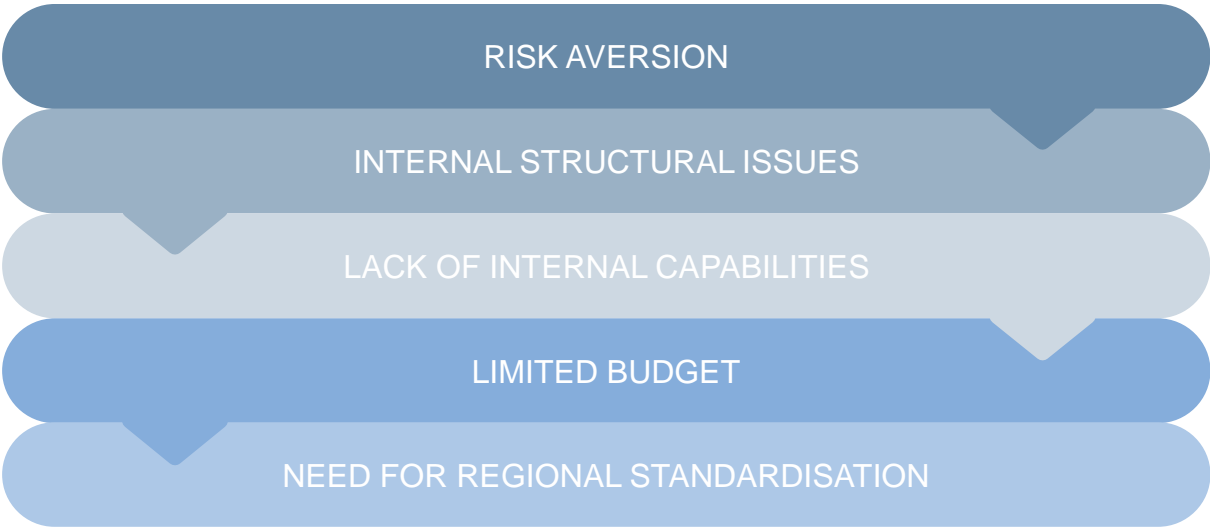
In addition, there were some further considerations that were specific to the size of the regulated institution. Many of the smaller institutions, such as challenger banks and niche insurers, noted that they had limited budgets for AML technology improvements and, as such, were looking for flexible pricing models from their suppliers. The larger institutions identified a completely different problem. Many operate in multiple jurisdictions across the globe and require a degree of standardisation across those jurisdictions, meaning that technology providers lacking a global reach were unlikely to be considered.

There were also differences in responses across industry sub-sectors. Within those sub-sectors where the nature of the financial products mean that customer interaction is relatively infrequent (such as life and pensions), technology is seen as being less beneficial as there is less of an overarching need. The reverse was true for areas such as retail banking which has much more frequent interactions with customers.

Finally, another key consideration related to the FCA. Many institutions felt that many of the supervisory and enforcement staff at FCA do

not have the technical expertise to appropriately evaluate the firms' adoption of new AML technology solutions. As a result, many firms felt that this would force them to potentially run new and old solutions in parallel, at considerable additional cost, as it may take additional time to prove the compliance of the new system to the regulatory authorities.

The diagram below highlights a number of the prominent challenges espoused by respondents:





Customer onboarding and maintenance

Role of technology in customer onboarding and maintenance

The vast majority of respondents across all sectors felt that customer onboarding and maintenance were two of the areas where technology offered the most promise, both in minimising operational costs and potentially improving the customer experience.

The use of AML technologies for customer onboarding and maintenance is seen as part of a broader shift towards digitisation, with a number of regulated firms making clear that a move to truly paperless working was a priority in the short to medium term.

Another theme emerging from the regulated firms was that the pace of regulatory change had often forced them to design new onboarding and maintenance processes in haste, with many of these processes proving to be expensive and inefficient.

A prominent example is in KYC where many operations were rapidly developed in response to regulatory change, rather than designed with operational efficiency in mind. Many perceived the emerging technologies in this area as a potential mechanism for correcting these inefficiencies and reducing operational costs, e.g. by automating elements of customer due diligence checks.

An overarching message from industry bodies, regulated institutions and a number of the technology firms concerned the perceived potential of 'utility' type models, whether government sponsored or from a third-party provider.

Many felt that this type of data sharing between regulated firms would deliver considerable benefits both in reducing costs and in preventing financial crime. A number of respondents went as far as to say that, given the proven nature of the supporting technologies underpinning utility services, such a move was very much a logical next step. More findings on utilities, including implementation challenges, are contained in the appropriate technology spotlight on page 33 of this document.

Existing technology landscape in customer onboarding and maintenance

Customer onboarding and maintenance is one of the parts of the AML lifecycle where regulated institutions already make use of technology solutions, many of which have been introduced in recent years. The most prominent of these technologies and their impacts included:

- Services from existing third-party data providers, including both specialist AML/KYC firms and those services provided by credit reference agencies. Most regulated institutions considered these services invaluable as part of their day to day operations. However a number also noted that they had previously experienced issues where the underlying data was not regularly updated, forcing them to make inaccurate decisions about customers.
- Many firms also noted that although some technology-driven service offerings were used the processes surrounding them were often manual – this was particularly prominent in both performing enhanced due diligence and adverse media searches, which were both considered labour-intensive by respondents.
- The use of biometrics has become prevalent in recent years, with a number of firms regularly using biometrics for customer maintenance purposes. A variety of use cases are currently adopted by regulated institutions, most prominently in performing ID&V activities or as an account access control.
 - Voice-based biometrics for telephony contact centres have been broadly adopted across Financial Services and are more recently starting to be adopted by life and pensions providers. These were perceived as particularly beneficial

in both improving the customer experience and in reducing fraud.

- Device-based biometrics for digital interactions with customers are becoming increasingly commonplace, particularly the use of fingerprint scanning. A number of regulated institutions opined that the technology for doing so was so widespread and low cost that it was perceived as commonplace by consumers. They also highlighted the benefits of the additional security and frictionless interaction from device based biometrics, rather than having to enter passcodes or equivalent.
- More complex biometrics have been introduced by a number of firms – including leveraging facial recognition technologies to match a self-taken photograph of a consumer to their passport. Other firms noted that it was an area for consideration but would require further analysis of the fraud/information security risk profile of the underlying technologies.
- A number of firms have begun the process of undertaking trials (in some cases relatively large scale trials) of industry utility models. This is often for defined activities within customer onboarding and maintenance, such as identity verification or document authentication. However, most respondents have noted that the complex barriers meant that these would not see widespread adoption anytime soon. More detail on industry utilities and their challenges is contained on page 32 of this document.

Emerging technology in customer onboarding and maintenance

A number of the emerging technologies in customer onboarding and maintenance are natural evolutions or expansions of existing technologies. Many respondents felt that the new technologies emerging in this space have the potential to be operationally transformative – particularly industry utility technologies that could significantly reduce the operational burden for regulated firms. These new technologies included:

- The continued expansion of utility technologies and KYC/AML data sharing across regulated institutions. Many felt that this would eventually become reality, although progress could be considerably accelerated by the interventions of either the regulator or the government more broadly.
- In addition, many respondents felt that the use of data analytics and machine learning within utilities could have an enormous positive impact in terms of identifying and preventing fraud, money laundering and terrorist financing. The pan-industry view of potential utilities would enable them to better spot trends and suspicious individuals/institutions. Unlike individual banks, they would have a clear view of the entire transactional profile of an individual within a jurisdiction. This benefit was considered to be particularly prominent in dealing with already high-risk products, sectors or services, such as correspondent banking or dealing with charities that operate in conflict zones.
- Many felt that advanced analytics technologies such as NLP would offer enormous operational benefits, particularly in fully automating currently manual processes, such as EDD and adverse media searches. The potential of the technology would allow these complex

areas to be less dependent on a human operator, rather than the current position where staff have to review adverse media items to determine if they are relevant.

- The views on blockchain for customer onboarding and maintenance were broadly consistent across the regulated firms. Whilst all felt that the technology has potential to be tremendously powerful and potentially transformative for Financial Services in general, they felt that no use case related to AML compliance had yet been demonstrated that was compelling. Moreover, a general lack of understanding of the technology both within regulated firms themselves and with the FCA, was seen as a barrier. This unusual juxtaposition (that people can think it both potentially incredibly useful, but not think of any specific uses) was repeated by a number of different respondents.
- Increasing use of device-based data, such as geolocation data from phones, was considered by respondents to be increasingly useful as part of a general move towards better behavioural and personal profiling of consumers, to create a truly bespoke approach to each consumer's individual risk profile – such as understanding usual locations, average movement patterns and other data.
- Video KYC is a technology that is relatively established and proven, but where uptake has been relatively slow. The consensus across regulated firms was that it has very specific use cases that are not appropriate for all providers. In particular, the view was that they are particularly useful in environments where customers do not have access to branches (such as remote areas or in some emerging markets) but that otherwise consumer appetite for the technology had been relatively low.

Challenges in embedding technology in customer onboarding and maintenance

Respondents articulated a number of views around the challenges hindering the development and embedding of new technology in customer onboarding and maintenance. Whilst many of these were technology specific, there were also a number of common issues identified:

- Many of the larger and more established institutions unsurprisingly made reference to legacy IT issues acting as a significant blocker on the usage of new technologies. This primarily came from two key issues:
 - Integration with legacy systems (in some cases dating back as far as the 1970s and 1980s) is often a significant challenge.
 - Data quality remains an enormous challenge – without significant data clean up exercises, much of the data quality inside a number of institutions is poor and could significantly limit the effectiveness of a number of new technology areas, such as utility technologies.
- Budget constraints were an almost universal theme across regulated institutions. Many suggested that already-compliant operational areas were often not a priority for additional investment – meaning that any new technology would need a particularly striking business case to be considered in favour of profit-driving activities.
- The notion of Reliance was also a common theme – many institutions felt that as long as the legislation prevented responsibility for AML activities being outsourced, the appeal of using third-party providers would continue to be low.
- The lack of guidance or leadership around new technologies in AML from the FCA or Joint Money Laundering Steering Group was also regularly cited as a hindering factor. Without explicit regulatory guidance (either from the FCA or JMLSG) around the use of new technologies and RegTech firms, regulated institutions are cautious in their approach to these new areas.
- In many regulated institutions, there is no one clear owner for technologies in AML. In many cases, the responsibility is split between compliance, technology and operational areas, slowing down decision making on adoption of new potential solutions.
- Data protection legislation was a pervasive theme across the entire AML lifecycle, with many regulated institutions feeling that increasing regulation in this area worldwide (particularly GDPR), made sharing customer data with any third party considerably less attractive. Whilst not linked solely to onboarding and maintenance, the growth of utility providers means it is potentially the area most impacted.

Lessons learned for firms looking to introduce technology in customer onboarding and maintenance

Respondents repeatedly highlighted two key lessons for firms thinking about introducing technology in this space:

- Many felt that engaging with the regulator early had proven helpful. Bringing the FCA along on the journey to implementation was felt to offer significant advantages over simply building a solution and then trying to convince the regulator it operated to the required standards after the event.
- Many highlighted that thorough due diligence should be undertaken on any potential supplier, particularly when considering the newer/smaller suppliers. A number of the regulated institutions cited examples where they had considered initially promising technologies only to discover they either did not work as advertised or failed to meet a key requirement, particularly in areas such as auditability, traceability and information security.



New technology spotlight

ELECTRONIC ID&V AND BIOMETRICS

Electronic Identification and Verification (EID&V)

EID&V was widely considered by respondents as one of the most mature and instantly useful elements of technology in AML, with many firms already using various mechanisms to meet their compliance obligations, including usage of third party data providers.

Many respondents felt that this was an area where a step change in operational performance could be easily achieved by the adoption of new technologies. Respondents placed a particular focus on using supporting technologies such as machine learning or NLP to achieve an uplift in efficiency in otherwise complex areas such as adverse media searches, enhanced due diligence or sanction/PEP screening.

Biometrics

For the majority of respondents, biometrics were firmly considered to be established technology, with many firms already using technologies such as fingerprint recognition, voice recognition and vein pattern recognition, primarily to authenticate existing customers and provide easy access to their accounts via digital and telephony channels.

A large number were also considering, or had begun, to adopt biometric technology for identity verification purposes, with photograph facial recognition and comparison technology becoming more widespread. However, some respondents felt that the fraud risks of such technology was not yet fully understood.

More complex biometric monitoring was also being considered by a number of respondents, particularly heartbeat monitoring – but the potential was considered to be limited by the availability and popularity of suitable devices.



Client screening

Role of technology in client screening

Client screening was an area where respondents were universally positive about the potential impact of new and emerging technologies on their compliance efforts. A number of potential applications were considered, including:

- Using better probabilistic matching and analytics technologies to improve the quality of the PEP/sanctions screening activities and better identify potential individuals and entities with a higher degree of certainty.
- Translation/transliteration technology was considered promising by firms operating in multiple jurisdictions, as it enables them to better process different languages and scripts.
- Advanced matching technologies, such as analytics-driven 'fuzzy matching' were considered to reduce reliance on (sometimes outdated) vendor data.
- A key use case for technology in client screening was around the reduction of false positives through analytics, machine learning and NLP. The processing of these false positives was stated by a number of respondents as their largest unnecessary manual overhead in AML compliance.

Existing technology landscape in client screening

The existing technology landscape in client screening is relatively simplistic, with almost all regulated institutions stating they used software to perform basic matching of customer names and other data against the necessary PEP and sanctions databases. A selection also used other technologies in this area:

- Many respondents were exploring data lakes/analytics proof of concepts to explore how they could potentially improve accuracy and reduce the volume of PEP/sanctions screening false positives that are generated.
- Others suggested that they also used third-party legal entity databases to minimise the operational overhead of identifying ultimate beneficial owners (UBOs) and controlling persons.

Emerging technology in client screening

Emerging technology for client screening is very much focussed on analytics, machine learning and NLP, with a large number of respondents trialling or considering trialling these technologies to reduce the need for manual false positive reviews – or even to remediate previously generated false positives.

In addition, the NLP element was considered particularly promising, as it could enable better processing of complex names with variable presentations or spellings, particularly where multiple languages or scripts were involved.

Many respondents also suggested that client screening would be easier if a pervasive national or international identity mechanism was established – although respondents believe that this is unlikely in the UK.

Challenges in embedding technology in client screening

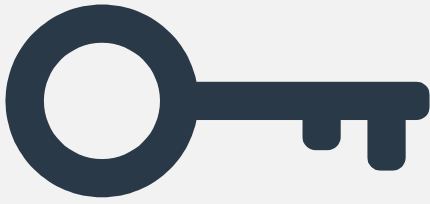
Many of the challenges articulated as relating to onboarding and maintenance in this document also apply to client screening. However, a few specific challenges were highlighted by respondents:

- Many respondents felt that the specific data associated with the names of their customers was poor enough to restrict the capability of new technologies in this space.
- A recurring theme was adoption of a low risk appetite for matching of names. Many firms want certainty on PEP/sanctions matches to minimise the potential of a negative customer experience.
- A number of regulated institutions felt that the regulatory burden and associated technical requirements in this space were relatively simplistic (i.e. checking customer names against agreed lists) and therefore felt that significant advantages could be gained by tweaking existing technology solutions, such as basic client screening systems. They felt that using new technologies such as NLP would represent a degree of overkill.
- Some smaller regulated institutions felt that the business case was not there for new technologies in client screening. Their lower customer volumes meant that far fewer alerts were generated, meaning that manual processing was not seen as a major overhead.

Lessons learned for firms looking to introduce technology in client screening

Specific lessons learned relating to client screening were not commonly provided by respondents.

The only recurring guidance in this area was to ensure that client screening activities, across all jurisdictions a firm may operate, in were fully aligned and that all languages, scripts and watch lists are considered prior to implementing anything new in this area.



New technology spotlight

BLOCKCHAIN

Blockchain was by far the most contentious of the new technologies explored during the course of this study. Opinions varied significantly across all types of respondents, with some considering it unimpressive while others believed it was the 'solution' to AML compliance – although it should be noted that this view was understandably more prevalent amongst technology providers.

From a theoretical perspective, the overall consensus was that distributed ledger technology has the potential to be transformative, both in AML compliance and across Financial Services more generally. During the course of this study potential uses were considered across every aspect of financial crime compliance. However, in

practice, the most common view espoused (from both technology and regulated firms) was that truly compelling blockchain use cases had yet to be articulated in AML compliance, restricting the pace of adoption.

In addition, respondents noted that there were a number of specific challenges hindering the adoption of the technology, the most prominent of which was the perceived knowledge gap. Respondents felt that a large number of compliance and technology staff in regulated institutions lack the technical expertise to truly consider a distributed ledger solution. Equally there is a view that the FCA lacks experience and capability in this area and firms appear reluctant to build a solution that the regulator might be unable to consider or approve.



Transaction monitoring and filtering

Role of technology in transaction monitoring and filtering

Transaction monitoring and filtering was one of the areas considered as having the most potential for the adoption of new and emerging technologies. With compliance in this space already predominantly technology driven, there is a widely held view that there are potential advantages.

Technologies in this area are used to monitor and filter transactions, preventing those that might go to sanctioned countries, entities and individuals and identifying those with a high risk of fraud or money laundering. New and emerging technologies are expected to provide the same fundamental activities but with greater accuracy, intelligence, speed and at a lower cost.

Existing technology landscape in transaction monitoring and filtering

The existing technology landscape in transaction monitoring and filtering predominantly consists of decision-tree based systems which work with defined rule sets to identify outliers (e.g. transactions of an unusual amount and in an unusual location) and trigger alerts. The nature of these rule sets and data quality issues mean that an enormous volume of alerts are generated, often requiring laborious manual review. This often results in true suspicious transactions only being identified sometime after the transaction itself has completed, in some cases many weeks after the fact.

The review of these alerts represents a significant operational overhead for firms, with many larger regulated institutions using substantial offshore operations just to process the alerts generated each day.

In addition, many of the more commonly used solutions are so-called black box solutions. The logic used within them is proprietary to the technology provider and often completely opaque to the regulated institutions, forcing them to perform lengthy testing exercises to collect the evidence that their engines are working in the manner intended.

Firms are actively trialling the usage of new technologies in this space – including analytics, machine learning and blockchain-driven solutions. The most common approach is to use these technologies alongside existing decision-tree based engines – often with the primary purpose of reducing the volume of alerts that need to be manually reviewed.

It should be noted that many of the more advanced transaction monitoring techniques were being trialled by wholesale banks as opposed to other Financial Services sub-sectors. These approaches were focussed on not just AML, but also on identifying and preventing other financial crime areas, predominantly market abuse.

Emerging technology in transaction monitoring and filtering

An enormous variety of new technologies are available to support transaction monitoring and filtering and many are being actively trialled or considered by regulated institutions. This was broadly considered the most innovative area of AML compliance, with technologies being considered including:

- Consolidation of data into data lakes, with associated analytics. This was one of the more common areas of focus; both technology providers and regulated firms felt that the sheer volume of data normally processed by transaction monitoring systems means that there is considerable scope for benefits to be delivered by unstructured searching and analytics. Practically, this approach has been considered in a number of different ways:
- Replacing existing transaction monitoring and filtering systems entirely, to undertake real-time transactional analysis.
- More commonly, working alongside existing systems, with a particular focus on reducing the volume of false alerts generated
- Machine learning within the data analytics options is a common consideration. Many firms believe that, if delivered successfully, it will enable them to build individual spending profiles for customers, to better identify potentially suspicious transactions. Alongside biometrics and other technologies, this could allow firms to produce true behavioural based monitoring.
- Blockchain or distributed ledger technologies have been widely considered, both at a single- and multi-institution level. Adoption remains at an almost universally early stage, but the technology is considered to show some early promise, particularly given its processing power and theoretical ability to meet the traceability and auditability regulatory requirements.

Challenges in embedding technology in transaction monitoring and filtering

Many of the more general challenges in embedding new technologies in AML apply to transaction monitoring, but a number of more specific challenges emerged from the responses across regulated institutions, technology firms and industry bodies, namely:

- Data quality, although a pervasive issue, is particularly prominent in transaction monitoring and filtering. Many firms stated that the number of false alerts generated by their existing systems is potentially more a result of data quality issues than any limitations of the current technology.
- As with other areas, firms are reluctant to fully replace their existing engines that have been accepted by the regulator – several suggested that an expensive replacement with new technologies would not be attractive whilst there was a risk of rejection by the regulator.
- It was felt that the potency of analytics and machine learning for analysing transactional data would be markedly improved if transactional data were shared across institutions, or if information on key trends was shared by law enforcement agencies.
- For many smaller institutions (or those with few heavily transactional products), the business case for new technologies in transaction monitoring and filtering just does not stack up. Limited volumes and complexity of transactions means that the benefit to be gained is, in some cases, felt to be minimal.

Lessons learned for firms looking to introduce technology in transaction monitoring and filtering

A number of respondents offered specific lessons for any firms considering new technologies in this space, including:

- Ensure a global view across jurisdictions is taken across an entire institution to prevent multiple solutions being built or considered.
- Collaborate closely with compliance, operations, technology and the regulator to ensure that the eventual solution meets all the necessary regulatory requirements.
- Ensure that any solution considered can scale sufficiently to handle daily transactional data.
- Ensure that any solution considers both AML/CTF and fraud aspects, to prevent expensive duplication.



New technology spotlight

DATA ANALYTICS, MACHINE LEARNING AND NLP

Data lakes and analytics

The usage of data lakes – large repositories of unstructured, multi-format data is increasingly commonplace across many Financial Services processes and AML compliance is no different. From an AML perspective, the technology is particularly promising in both client screening and transaction monitoring – two areas where traditionally large amounts of either false positives or erroneous alerts have been generated, with a significant associated operational cost. It is also widely understood with the majority of regulated institutions, who contributed to this study, either actively using or strongly considering using data lakes and some form of analytics.

Perhaps the biggest potential value is in the transactional space; the ability of modern analytics to identify otherwise invisible trends across large data sets lends itself ideally to both the prevention of fraud and money laundering.

Machine learning

Machine learning was regularly cited by respondents as one of the most promising technologies in AML compliance – particularly in its ability to dramatically enhance the performance of existing analytics or decision-based solutions by ensuring each iteration is more effective than the last.

Most prominently, it can be used alongside transactional, onboarding and mobile device-based data to form true behavioural profiles for each customer – allowing a new standard in fraud and money laundering detection.

Natural Language Processing (NLP)

NLP was one of the emerging technology areas with the greatest potential for transforming previously manual operational activities. In particular, areas such as enhanced due diligence or adverse media searches have traditionally been at least partially performed by operational staff, due to the interpretation required to make decisions about often complex cases. The development of NLP technologies means that not only can

that interpretation be automated, significantly reducing operational cost, but it also could improve consistency of decision making.

The other area with potential NLP applications is client screening – where matching of names with different spellings, formats or scripts has always caused challenges for traditional matching systems. Adopting NLP technology could potentially enable both a reduction in false positives and better prevention of both fraud and money laundering/terrorist financing.



Reporting and management information (MI)

Role of technology in reporting and MI

Traditionally, technology has played a limited role in reporting to both the regulator or other bodies such as the local Financial Intelligence Unit (FIU). For most regulated institutions, the production and filing of suspicious activity reports (SARs) in the UK has been an entirely manual and administrative function, with little in the way of automation or technology.

However, new and existing technologies could offer considerable advantages and operational improvements to regulated firms in this area. In particular, data analytics and machine learning technology has the potential to rapidly reduce the number of potential SARs needing human review or intervention, significantly reducing operational costs.

Furthermore, modern smart workflow tools have the ability to automatically transfer SARs to FIUs in some jurisdictions where file formats have been agreed, preventing the need for manual controls and hand-offs.

MI is an area where new technologies have achieved a step change in performance in recent years, with data visualisation now relatively commonplace in supporting front office activities such as product sales. Unstructured data analysis and data visualisation now provide greater insights and accuracy than may have been available via traditional methods, with some firms beginning to gain insights into their SAR production over an extended period.

Existing technology landscape in reporting and MI

The usage of reporting technology was relatively limited for most regulated respondents, with many suggesting that reporting was predominantly a manual process for their organisations.

However, a number admitted that they were increasingly using technologies in this area, for two primary purposes:

- To use analytics and machine learning to reduce the volume of SARs needing human intervention.
- To use newer workflow tools to better track the progress of SARs, particularly with regards to regulatory SLAs and where communications or reports have been shared with other regulated institutions. This enables clearer and quicker collaboration between firms and increases the chances of stopping the flow of illicit funds.

Almost all respondents suggest that they had explored and regularly used existing advanced MI tools, including data visualisation. However, most suggested that using it for FIU reporting and/or AML operations was a lower priority, despite its potential, as revenue-generating areas were the priority for any such investment.

Emerging technology in reporting and MI

Many of the emerging technologies mentioned in this report have potential in the reporting and MI space, particularly in the production, review and monitoring of SARs. The overwhelming view from respondents was that data analytics, machine learning and even NLP technologies could have a significant benefit in automating SAR production and reducing the amount of potential suspicious activity alerts that need to be considered.

From an MI perspective, the continuing evolution of data interrogation and visualisation technology is particularly promising, with many respondents feeling that it could eventually be transformative for their management of operational MI in general, and particularly in the AML space. In particular, many respondents noted that their AML MI was often very operational in nature (often duplicating formats and metrics from call centres and other operational areas), and felt that newer mechanisms would be able to give them both customer and compliance insights.

Challenges in embedding technology in reporting and MI

Many of the challenges experienced in embedding new technologies into other areas of the AML lifecycle are equally applicable to reporting and MI. In particular, data quality remains a substantial issue – particularly in generating maximum benefit from MI. Many respondents stated that MI-related trials, particularly on SARs, had failed in the past as the poor quality of data prevented them from gaining any real insight.

One particular challenge that was regularly articulated around reporting and MI was the difficulty of creating a compelling business case for new MI solutions. Many felt that reporting and MI was often de-prioritised in favour of other more prominent areas of the AML lifecycle. In particular, a key reason cited was that investing in other areas of technology instead, such as customer onboarding or transaction monitoring can generate additional customer insights that could be potentially be used for cross-selling purposes.

Finally, a further challenge around automated reporting from many respondents relates to the readiness of the local FIU to accept automated reports. Many felt that the lack of clearly defined standards and transfer mechanisms to FIUs was a disincentive to move forward in this area.

Lessons learned for firms looking to introduce technology in reporting and MI

Very few lessons learned were provided by respondents that were specific to reporting and MI. The one recurring element from respondents was that it is imperative to move away from a paper-based model to achieve true operational efficiency and control.



New technology spotlight

INDUSTRY UTILITIES

Industry utilities (mechanisms for sharing KYC, transactional or other data between institutions through a third party) were considered one of the most attractive areas by the majority of respondents, for a number of different reasons.

By sharing AML compliance activities across multiple institutions, the widespread view is that significant cost efficiencies could be achieved, as well as allowing the third party to better identify systemic trends – including pan-institutional trends in fraud, money laundering, or terrorist financing.

A majority of participating regulated institutions had trialled the usage of utilities, but most felt that there were significant challenges that were slowing the adoption of utilities on a widespread basis.

Most prominently, it was felt that, without a density of regulated institutions becoming fully aligned behind an approach, it would require intervention from a regulator or trade body to make it a reality. This could be done either through mandating standards or through establishing a forum across regulated institutions and technology firms to facilitate the ongoing discussion.

In addition, other significant challenges were articulated by regulated firms, including ever-expanding data privacy legislation and existing legislation on reliance preventing the outsourcing of responsibility to the third-party provider in question.

**BREAKING
DOWN BARRIERS**
THE VIEW FROM
TECHNOLOGY PROVIDERS



Background to the topic

In recent years, the development and use of Financial Services compliance technology has expanded enormously on a global basis. This has been particularly true in geographies like the UK with strong Financial Services centres and where support has been provided by governments and regulators. A wide range of technologies and providers have emerged, with potentially disruptive and additive consequences for the established Financial Services firms. A good example of the latter in particular are the newer RegTech providers, focussing on regulatory compliance technology to support regulated institutions.

For the purposes of this study, we considered technology firms to include start-ups, medium sized companies, large companies and even regulated institutions themselves that create and potentially distribute financial services technology.

Focus of the section

During the course of this study, we spoke with over 20 selected technology providers across a range of company types and technologies, to gather their views on both the AML technology landscape and the FCA's approaches to innovation in this sector.

This particular section focusses on the recurring themes emerging from the providers – particularly around their perceived barriers to success and their perceptions of the collaborative landscape between regulated institutions and technology providers.

Overall conclusions

Overall, technology providers felt that they were well placed to succeed in the AML compliance space, although they noted that there were still a substantial number of barriers to both entry and success. These barriers varied across a number of areas, including regulatory, economic and operational – with each provider tending to see different areas as the biggest barrier to their success.

Barriers facing AML / KYC technology firms

Challenges preventing Financial Services institutions adopting AML / KYC technology

Many of the technology providers felt that getting major Financial Services institutions to adopt new technologies was a significant challenge – with smaller providers particularly concerned. Some of the common challenges articulated include:

- Larger banks have established arrangements with large providers and are reluctant or unwilling to shift to a new provider.
- Many regulated institutions were perceived as having a low risk appetite in this space, with many viewing the risk of using unproven emerging technologies as too high – both from a regulatory and operational perspective.
- A number of the technology providers felt that the view from regulated institutions was that the providers did not understand the regulatory environment – a perception that they felt was unfair. That said, a number also felt that the changing regulatory environment itself was fundamentally a challenge; many of the smaller providers said they did not have the bandwidth or resources to perform robust horizon scanning for regulatory changes.
- One of the largest perceived barriers was scale. A number of smaller providers felt they would be unable to handle more than one major client, with even larger firms sometimes struggling to match the geographic reach required by clients.
- Finally, a key blocker cited by many technology providers was that regulated firms often had no clear buyer for AML technologies. They felt that there was a recurring disconnect between IT and operations staff who might see the value and the eventual compliance buyer who may not understand the solution.

Challenges developing new AML / KYC technology solutions

Most respondents were positive about the general landscape in the UK for developing new AML technology solutions, with few feeling there were fundamental impediments to their success. However, a few recurring elements were identified as significant challenges, namely:

- A lack of agreed or mandated standards across a variety of elements including data security and identity verification requirements - meaning that providers were often working to different standards to their potential clients.
- A perception that, whilst individual technologies may prove valuable, an

unwillingness by individual firms to share insights and workings meant that the creation of a true ecosystem was impossible. One respondent suggested that the AML technology landscape resembled a 'black box swamp'.

- Many felt that increasing data privacy considerations were preventing the development of more efficient and cheaper options for analysing data.
- A number of respondents felt that FCA and their initiatives in this space – such as the Sandbox – were undersized compared to demand and therefore unfairly favouring those providers who managed to secure access.

Wider industry challenges facing AML technology firms

One of the key focus areas that drew the widest range of responses, particularly from the smaller more entrepreneurial providers, related to the wider industry challenges facing firms intending to operate in the AML technology space. Some of the more common challenges mentioned included:

- The lead time for designing, developing and testing new regulatory technology remains lengthy due to the need to continually assure compliance. This means that start up services or products in this space require significant investment beyond normal technology projects.
- Many smaller technology firms spoke openly of a fear of contagion risk. They felt that the perceptions of them by regulated institutions was relatively low, and that if even one was to be found noncompliant or have an issue such as a data breach, it would erode confidence in the providers as a whole.
- Data was a significant thematic issue, both in terms of the security/protection elements inherent in any sharing of data, but also in terms of the challenges of working with volumes as large as those found in major

Financial Services institutions, particularly in the transactions space.

- The concept of identity was one widely discussed across a number of respondents. Many felt that without a functioning government digital identity service, adoption in Financial Services would be slow at best. Others felt that without clear standards and definitions being laid down by a government body or a regulator, it was a difficult area in which to build technology. Respondents also highlighted some systemic issues with the increasing push towards a consolidated digital identity mechanism, including:
 - Increasing data privacy awareness in the UK meaning that significant volumes of people may choose to opt out of any scheme.
 - A widespread move to an all-encompassing digital identity scheme may make it harder for exceptional cases such as the unbanked to gain access to financial services.

Collaboration across entities

Respondents across the technology providers noted that collaboration was essential to their ongoing development, particularly as they felt collaborations were more likely to be considered by regulated firms. Many also noted that it allowed the development of partnerships to provide solutions across the entire AML lifecycle. The most common collaborations included:

- Involving themselves heavily with Financial Services or technology forums.
- Working with other similar providers to form a wholesale 'utility' type offering.
- Working with integration providers such as consultancy firms to provide a more complete design and delivery solution.

- Engaging with supporting technology partners, such as infrastructure or cloud providers, to enable their services to be sold as 'turnkey' solutions that can be implemented as is.
- Collaborating with consultancy firms or think tanks to formulate research around their proposed focus areas.

A small number chose not to widely collaborate, preferring to badge themselves as agnostic to supporting infrastructure technologies or even other technology solutions.

**‘A GOOD START,
BUT MORE TO DO’
INDUSTRY VIEWS ON THE
FCA’S APPROACH TO NEW
TECHNOLOGIES IN AML
COMPLIANCE**



Background to the topic

Finding out respondents' perceptions of the FCA and its approach to innovation in AML was a key focus area of this study, both in terms of views about its historic approach to this subject and ways in which it may be able to improve in future.

Focus of the section

This section focusses on the view of respondents across regulated institutions, technology firms and other bodies on the FCA. In particular, the focus was on ways in which the FCA could further innovation in AML as well as a comparative view against regulators in other jurisdictions.

Overall conclusions

Overall, the view of the FCA from respondents was almost universally positive, in terms of the FCA's approach and execution of that approach in the AML space. Most respondents recognised that this was a complex area and that encouraging innovation was a difficult aim for a regulator to achieve. Most also felt that the regulator generally compared favourably with those in other jurisdictions, and was generally perceived to be a front-runner in adapting where necessary. Many respondents in particular praised the Sandbox and other initiatives as being particularly welcome.

However, respondents stressed that there was still a large amount more that could be done by both the FCA and other regulatory or governmental bodies to encourage new technologies in AML – both in terms of enhancing and updating regulations as well as potentially facilitating future discussions.

Steps FCA could take to further innovation within AML

In general, the feedback from respondents was positive about the FCA and its approach to innovation in AML, with many citing the FCA's willingness to embrace new approaches and directly facilitate innovation via the Sandbox and other mechanisms as positive steps. However, many felt that there were a number of areas in which the FCA could take additional steps to further encourage innovation in this area.

Firstly, many felt that there were significant alignment issues within the FCA itself and the messages being provided to the marketplace. In particular, respondents pointed to differing approaches taken by general supervisory, AML policy and AML enforcement teams, with many feeling that messages from the policy teams around openness to innovation were not always reflected by supervision staff performing reviews of the firms.

In addition, there was also a perceived disconnect between the FCA and other government institutions such as the Treasury (HMT), particularly in areas such as sanctions. The overarching preference from respondents was for one set of regulations and guidance on potentially overlapping areas such as AML and sanctions. Many also felt that there was more that could be done by these institutions to support AML compliance – in particular, many respondents articulated a desire for greater communication around trends and findings from the NCA.

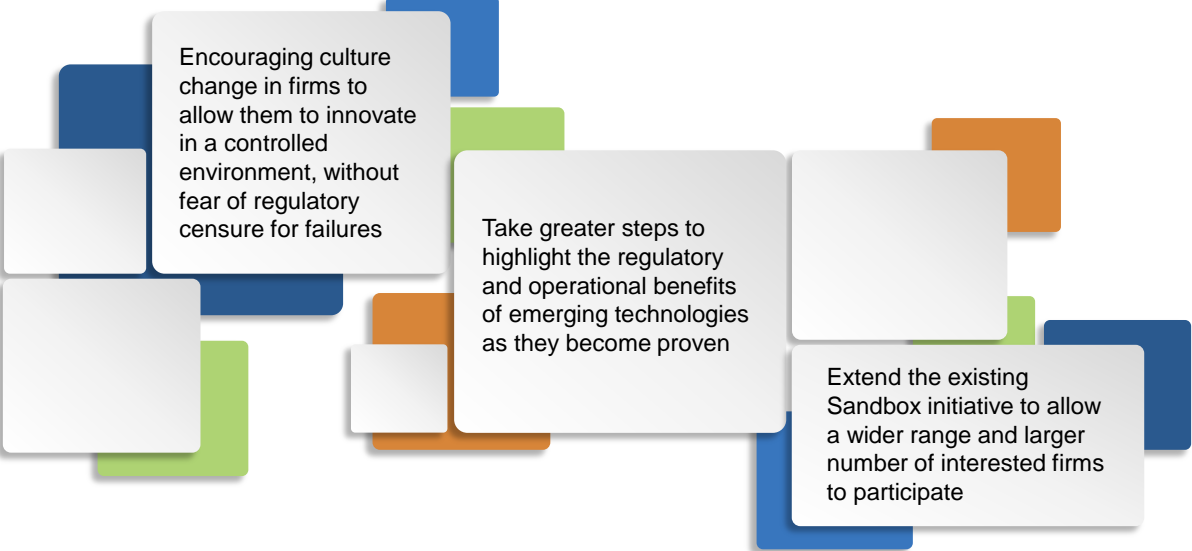
Secondly, it was felt by a majority of participants in the study that the FCA or another governmental body would have to take steps to make widespread industry utility adoption or data sharing between institutions a reality.

Many felt that achieving a truly unified view of an approach to shared KYC in the near future would be impossible without the FCA or another body either directly mandating an approach/standards or facilitating a potential forum amongst regulated institutions and technology providers to enable them to agree on a way forward.

Many respondents also expressed their frustration with the progress of the `verify.gov` scheme. They felt that it had not progressed as expected and had potentially hindered the creation of other identity solutions as many regulated institutions had believed it might eventually be mandated. Whilst not an FCA initiative, a number of participants expressed a desire for guidance or a positioning statement from the FCA (albeit a number acknowledged that this was unlikely).

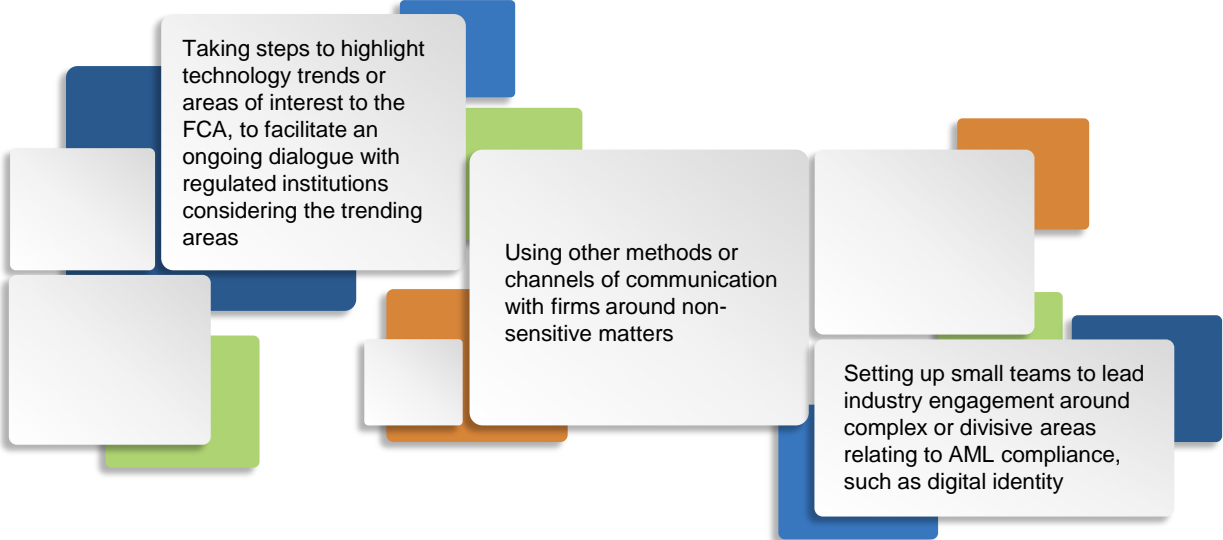
Another key theme was that many respondents felt that the FCA was uniquely placed to encourage more collaborative innovation in Financial Services, either by establishing more forums for frank discussions between industry participants, or by expanding the range of Sandbox-like services to let regulated firms trial new and innovative approaches to compliance. This could include the extension of the Sandbox to encompass other governmental areas such as HMT or the Home Office.

In particular, one area mentioned was that a Sandbox-like initiative would be perfect for larger-scale industry utility trials. Others also felt that the FCA would be well placed to showcase promising new technology and promote a broader innovation culture through a variety of mechanisms, including:



A number of participants also felt that the FCA could do more in terms of communicating with the industry, including more informal methods of communication. Some of the more common suggestions are shown below:

Finally, a number of participants recommended that the regulator take additional steps to upskill their staff around new and emerging technology. This would enable a more rapid and accurate assessment of new approaches, but also build confidence amongst industry participants that the FCA will be able to effectively review their new technology approaches once built.



Differences between UK and other jurisdictions' approach to AML / KYC innovation

Most respondents positively reviewed the FCA compared to regulators in other jurisdictions; this was particularly prominent amongst the multi-national institutions participating in the study. A repeated theme was that the FCA was widely viewed as the front-runner regarding innovation in AML, with many other regulators across the globe observed as following the FCA's lead, particularly with regards to tangible activities such as the Sandbox initiative.

There were a variety of differing perceptions around regulatory approaches to technology providers. A number of providers expressed frustration on the differences in approach between jurisdictions, feeling that it hindered the arrival of new entrants across borders. In particular, some firms cited differences in regulations around data protection, data security and identity verification as particular areas in which it is difficult to deliver a compliant solution across jurisdictions.

However, some respondents welcomed a more domestic approach, with a number encouraging efforts in some local jurisdictions (such as the UK) to accelerate the growth of new start-ups, feeling that it was a welcome boost to local industry.

The one prominent area of comparative criticism was around the speed of regulatory approval of new RegTech firms, which was considered to be extremely slow in the UK. Many respondents felt that this was an area where the UK lagged considerably behind other European and global regulators.




APPENDIX 1: LIST OF INTERVIEWED PARTIES

Company Name	Date interviewed
Anonymous Academic Institution	19 Jan 17
Anonymous Regulated Firm	16 Dec 16
Anonymous Regulated Firm	22 Dec 16
Anonymous Regulated Firm	18 Jan 17
Anonymous Regulated Firm	19 Jan 17
Anonymous Regulated Firm	23 Jan 17
Anonymous Regulated Firm	31 Jan 17
Anonymous Regulated Firm	01 Feb 17
Anonymous Regulated Firm	06 Feb 17
Anonymous Regulated Firm	10 Feb 17
Anonymous Regulated Firm	22 Feb 17
Anonymous Technology Firm	19 Jan 17
Anonymous Technology Firm	31 Jan 17

Company Name	Date interviewed
Atom Bank	19 Jan 17
AU10TIX	14 Feb 17
BAE Systems	16 Dec 16
BasisTech	20 Dec 16
BBA/JMLSG	23 Jan 17
Behavox	17 Feb 17
Cardabel	28 Feb 17
Clydesdale Bank	27 Jan 17
Cynopsis Solutions	23 Jan 17
Encompass	19 Jan 17
Experian	12 Dec 16
Government Digital Service	19 Jan 17
Hellosoda	15 Dec 16
HSBC	20 Dec 16
ICICI Bank	24 Jan 17
Innovate Finance	23 Jan 17
miiCard	26 Jan 17

Company Name	Date interviewed
MLRO Forum	25 Jan 17
ObjectTech	16 Dec 16
Paycasso	11 Jan 17
RUSI	11 Jan 17
Salviol	12 Jan 17
Scottish Financial Enterprise	12 Jan 17
Sparkl	25 Jan 17
Swift KYC	15 Dec 16
Sybenetix	11 Jan 17
Tandem	18 Jan 17
Thompson Reuters	19 Jan 17
TISA	03 Mar 17
Tradle	16 Dec 16
Trustev	13 Feb 17



APPENDIX 2: LIST OF KEY FOCUS AREAS

As part of this review, a number of key focus areas were identified to answer the key questions. These were as follows:

Key Focus Area	Secondary Focus Area
Innovative decision making	Regulated firms' internal decision making process when considering the adoption of new technologies within the AML lifecycle
Customer onboarding and maintenance (including ID&V etc.)	The role current AML technologies play in regulated firms' customer onboarding and maintenance operations
	The role future AML technologies could play in regulated firms' customer onboarding and maintenance operations
	How AML technologies improve regulated firms' customer onboarding and maintenance operations
	Sharing customer data with other institutions (e.g. a third-party due diligence utility) or neighbouring regulated institutions
	The challenges regulated firms face in introducing/embedding AML technologies focussed on customer onboarding and maintenance operations
	The existing technology landscape across customer onboarding, including a view of the types of technology and prominent providers
	The challenges technology firms face in furthering their customer onboarding and maintenance innovations

Guidance to regulated firms seeking to introduce AML technologies to improve the efficiency of their customer onboarding/maintenance processes

The steps the FCA could take to encourage further innovation within the customer onboarding and maintenance focussed parts of regulated firms' lifecycles

**Client Screening
(PEPs/Sanctions)**

The role current AML technologies play in regulated firms' client screening operations

The role future AML technologies could play in regulated firms' client screening operations

How AML technologies improve regulated firms' client screening operations

The challenges regulated firms face in introducing/embedding AML technologies focussed on client screening operations

The existing technology landscape across client screening operations, including a view of the types of technology and prominent providers

The challenges technology firms face in furthering their client screening innovations

Guidance to regulated firms seeking to introduce AML technologies to improve the efficiency of their client screening processes

The steps the FCA could take to encourage further innovation within the client screening focussed parts of regulated firms' lifecycles

**Transaction
Monitoring/Filtering**

The role current AML technologies play in regulated firms' transaction monitoring/filtering operations

The role future AML technologies could play in regulated firms' transaction monitoring/filtering operations

How AML technologies improve regulated firms' transaction monitoring/filtering operations

The challenges regulated firms face in introducing/embedding AML technologies focussed on transaction monitoring/filtering operations

The existing technology landscape across transaction monitoring/filtering, including a view of the types of technology and prominent providers

Sharing customer data with other financial institutions/a neighbouring regulated institution for transaction monitoring/filtering purposes

The challenges technology firms face in furthering their transaction monitoring/filtering innovations

Guidance to regulated firms seeking to introduce AML technologies to improve the efficiency of their transaction monitoring/filtering processes

The steps the FCA could take to encourage further innovation within the transaction monitoring/filtering focussed parts of regulated firms' lifecycles

Reporting/MI

The role current AML technologies play in regulated firms' reporting

The role future AML technologies could play in regulated firms' reporting

How AML technologies improve regulated firms' reporting

The challenges regulated firms face in introducing/embedding AML technologies focussed on reporting

The existing technology landscape across reporting, including a view of the types of technology and prominent providers

The challenges technology firms face in furthering their reporting innovations

Guidance to regulated firms seeking to introduce AML technologies to improve the efficiency of their reporting processes

The steps the FCA could take to encourage further innovation within the reporting focussed parts of regulated firms' lifecycles



APPENDIX 3: GLOSSARY

AML	Anti-Money Laundering – those activities undertaken by governmental bodies, law enforcement and Financial Services institutions to prevent money laundering.
Biometrics	Biometrics are key personal physical metrics that can be used to identify an individual.
Blockchain	A blockchain is a type of database built on distributed ledger technology, with data stored in ordered records called 'Blocks'.
CDD	Customer due diligence – those activities undertaken by a Financial services institution to understand the risk profile of any given customer.
CTF	Countering Terrorist Financing - those activities undertaken by governmental bodies, law enforcement and Financial Services institutions to prevent the financing of terrorism.
Distributed Ledger	A distributed ledger is one where storage elements are not attached to a single processing unit, often being spread across multiple physical locations.
EDD	Enhanced due diligence – those additional activities undertaken by a Financial Services institution to understand the risk profile of high-risk customers.
FCA	Financial Conduct Authority – The FCA is one of the UK's primary Financial Services regulatory bodies, with three main roles: Protecting Consumers, Enhancing Market Integrity and Promoting Competition.

GDPR	General Data Protection Regulation – an EU regulation designed to strengthen/standardised data protection controls across in-scope jurisdictions.
HMT	Her Majesty's Treasury - HM Treasury is the UK government's economic and finance ministry, maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth.
ID&V	Identification and Verification – The collective term for those activities mandated for regulated institutions to identify their customers.
Industry Utilities	Industry Utilities are those service/technology providers offering a centralised outsourcing of key common tasks, potentially across an entire industry.
JMLSG	The Joint Money Laundering Steering Group –The JMLSG is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations
KYC	Know Your Customer – those mandatory activities undertaken by Financial Services institutions to understand their customers and associated risk profile.
Machine Learning	Machine learning refers to those mechanisms that allow computers to learn without being explicitly programmed by humans.
NCA	The National Crime Agency is the UK's law enforcement and government body dedicated to tackling serious and organised crime. The NCA is also the UK's Financial Intelligence Unit.
NLP	Natural language processing – those mechanisms that allow computers to better understand and interact with naturally spoken 'human' languages.
PEP	Politically Exposed Person – those individuals (or entities) considered to have a degree of political exposure and therefore a higher potential risk of financial crime.

Sanctions

Sanctions in the context of this report refer to economic or political blocks on trade or transactions enforced on either countries, institutions or individuals.

SARs

Suspicious Activity Reports – the mechanism by which Financial Services institutions report unusual activity to relevant Financial Intelligence Units.



APPENDIX 4: SUMMARY TABLE OF TECHNOLOGIES

Technology	Description	Illustrative example of how it may aid AML compliance	Respondents' views: is it proven in practice?	Respondents' views: challenges to implementation
Biometrics	Using biometrics (including via mobile devices) such as fingerprints, iris recognition, vein mapping and voice recognition to identify customers.	Biometrics have particular promise in the customer onboarding and maintenance space – particularly for authenticating ongoing customer interactions.	Respondents felt that biometrics represented proven technology, although with a potential heavy reliance on mobile devices.	Respondents felt that the biggest challenge to implementation was around difficulties in securing the registration step when using mobile-device based biometrics.
Blockchain	Using distributed ledger-based database technology for a variety of potential use cases.	Blockchain has a variety of theoretical use cases in aiding AML compliance, with some of the most promising being in the transaction monitoring space.	Respondents felt that the technology was proven at a fundamental level – but there was widespread scepticism over whether the 'right' use case has been identified.	Respondents felt that there was a lack of compelling use case for the technology; the technology was considered opaque and 'hard to sell'.
Data Analytics and Machine Learning	Using advanced analytics and machine learning capabilities to process large volumes of data in an accelerated timeframe, with continuous improvement.	Analytics and machine learning have a number of different applications; many of the most promising involve using these systems for transaction monitoring for more complete analysis of unusual transactions, potentially in real time.	Respondents felt that analytics/machine learning were widely used and proven technology areas, albeit evolving constantly.	Respondents felt there was sometimes a lack of business case to move away from existing solutions, and that data quality remains a substantial limiting factor.
Geolocation	Using a customer's location data to determine a behavioural profile/support financial crime compliance activities.	Geolocation technology can be used in a multitude of ways, including: verifying a customer's location matches a recognised address, creating a behavioural profile for transaction monitoring purposes and more.	Respondents felt that the technology was proven, although noted that accuracy can vary by device.	Respondents felt that using and collating the device data in real time can be a challenge, as can the broader data privacy implications.

Technology	Description	Illustrative example of how it may aid AML compliance	Respondents' views: is it proven in practice?	Respondents' views: challenges to implementation
Industry Utilities	Third-party service/technology providers offering the wholesale outsourcing of various compliance activities across a whole industry.	Industry Utilities were most commonly considered for CDD/ID&V purposes, although could theoretically work across the AML lifecycle.	Respondents felt that the technology was generally proven, although adoption in many geographies (including the UK) has been slow	Respondents felt there were a number of significant challenges to widespread adoption, including a lack of clear standards and low risk appetites meaning regulated firms were often unwilling to outsource these activities.
NLP	Natural Language Processing encompasses technologies that can mimic or analyse human speech/languages.	NLP has various AML compliance use cases; many of the more prominent relate to enhanced client screening capabilities, including name translation/transliteration.	Respondents felt that the technology was broadly proven although still evolving. They felt that functionality was proven to a greater extent for more simplistic-tasks rather than full language replication/analysis	Respondents felt that the technology potentially lacks effectiveness in more complex areas of analysis, although noted this was continually evolving.
Video KYC	Performing KYC checks over a video link to enable remote gathering of information	Video KYC is perceived as allowing the benefits of in-person customer interactions without requiring a branch network, particularly for performing customer onboarding related compliance activities.	Respondents felt that Video KYC technology was generally proven.	Respondents felt that there was no broad desire for the functionality from consumers, no clear consensus on which underlying technology to use, and often minimal advantages over existing digital interactions.
Workflow Tools	Advanced workflow tools provide combination workflow, case management and MI tools to control and support various operational activities.	Workflow tools have a number of AML compliance use cases. Common uses include in customer onboarding to create a single KYC 'file' as well as in SAR production/analysis/reporting.	Respondents felt that the technology was both proven and readily available.	Respondents felt that it was often challenging to put forward a compelling business case, with other technologies perceived as providing greater tangible benefits, either in terms of financial crime prevention or cost reduction.



CONSULTING
TECHNOLOGY
INNOVATION

We Make the Difference

An independent firm of over 2,600 people, we operate globally from offices across the Americas, Europe, the Nordics, the Gulf and Asia Pacific.

We are experts in consumer and manufacturing, defence and security, energy and utilities, financial services, government, healthcare, life sciences, and transport, travel and logistics.

Our deep industry knowledge together with skills in management consulting, technology and innovation allows us to challenge conventional thinking and deliver exceptional results that have a lasting impact on businesses, governments and communities worldwide.

Our clients choose us because we don't just believe in making a difference. We believe in making *the* difference.

Corporate headquarters

123 Buckingham Palace Road
London SW1W 9SR
United Kingdom
+44 20 7730 9000

paconsulting.com

This document has been prepared by PA. The contents of this document do not constitute any form of commitment or recommendation on the part of PA and speak as at the date of their preparation.

**© PA Knowledge Limited.
All rights reserved.**

No part of this documentation may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise without the written permission of PA Consulting Group.