Deloitte.

Joining the dots
An integrated approach to tackling financial crime

A Deloitte Analytics Institute paper

Contents

Executive summary

An integrated approach to tackling financial crime improves risk management and customer service.

The pressure to tackle financial crime has never been greater. But tightening regulation, growing demands by customers for integrity in firms' financial dealings and increasing criminal sophistication are combining to create a perfect storm for the financial services sector. Yet current approaches remain a patchwork of fragmented, inefficient, inflexible and, ultimately, ineffective efforts designed around a discrete set of compliance chores.

In times of continuing economic uncertainty, it may seem easier to take the path of minimal compliance rather than trying to change. However, firms need to invest in bringing their data together to create an integrated approach to financial crime. Such an approach will align all business capabilities, including strategy, people, processes, technology and data, towards a more unified view of risk.

An integrated approach, with data and analytics at its heart, will help firms improve their financial intelligence and reduce costs. The insights they extract from their data will not only allow financial crime teams to fulfil their regulatory obligations, they will also be able to join the dots in criminal activities that would otherwise have remained undetected. The insights will also help improve customer services as all customer-oriented activities begin to exploit the synergies in the approach.

Only by folding discrete approaches, such as Anti-Money Laundering (AML), anti-bribery and counter-fraud, into the larger mosaic of enterprise risk and performance management can firms begin to align their financial crime capabilities with other risk and regulatory activities. This will then set the stage for increased business value and improved service performance in a set of activities that the business has traditionally seen only as a cost and compliance centre.

Can financial institutions comply more effectively and efficiently?

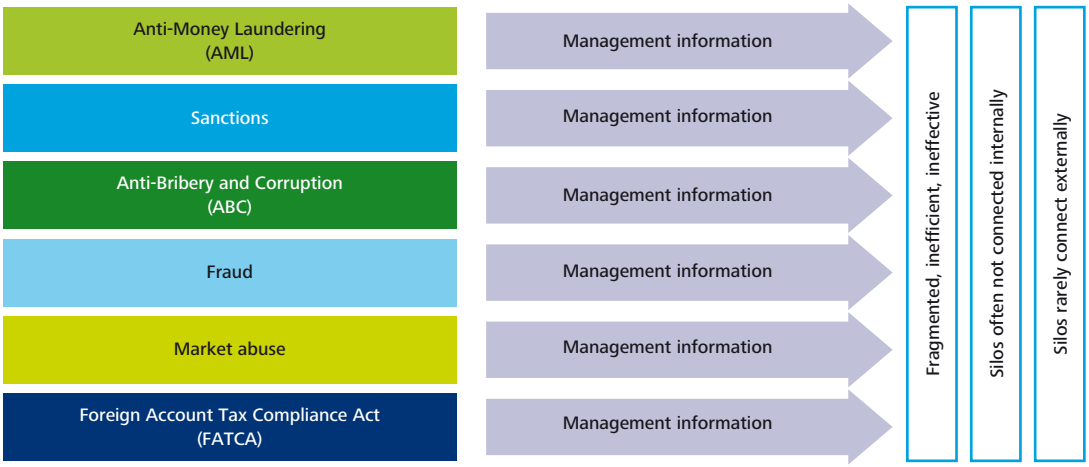
A perfect storm for the financial services sector

According to the Financial Services Authority (FSA), financial crime includes *"… any offence involving money laundering, fraud or dishonesty, or market abuse."*[1] Although it would seem easy to dismiss financial crime as a purely 'white collar' issue based on this rather clinical definition, many other types of crime are motivated or fuelled by money. In a speech to the annual FSA Financial Crime Conference back in 2005, Sir Callum McCarthy, former Chairman of the FSA, talked about the role financial institutions needed to play in curbing a much wider web of crime. He said, *"It is about us all playing our part in the fight against drug and people trafficking, terrorist financing and other only too real social problems. It's about the social consequences of those crimes. It's about fighting the harm on our streets that affects all members of society – including the financial services sector."*[2]

Over the last 10 years, the imperative to fight crime has meant that firms in the financial services sector have been subject to ever-tightening regulation and legislation, including the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007, the Bribery Act 2010 and the constantly changing UK sanctions regime. Guidance from the FSA also requires firms to *"conduct their business with integrity and with due skill, care and diligence, and to take reasonable care to organise and control their affairs responsibly and effectively with adequate risk management systems."*[3] Adherence to this guidance not only helps in the fight against financial crime but also helps to build trust and reputation with customers.

Compliance on its own does not control the criminals, of course. And criminals are nothing if not increasingly innovative. In a world where everything and everyone has a digital connection, crimes are growing in subtlety and sophistication, and are becoming much harder for firms and the law enforcement authorities to spot.

Figure 1. Current siloed approach to managing financial crime



In a world where everything and everyone has a digital connection, crimes are growing in subtlety and sophistication, and are becoming much harder for firms and the law enforcement authorities to spot.

But current approaches to financial crime are a patchwork

Despite guidance from the Joint Money Laundering Steering Group (JMLSG) suggesting that firms need to have *"close liaison"* between those responsible for tackling fraud, market abuse, money laundering and terrorist financing, current approaches remain a patchwork of fragmented, inefficient and, ultimately, ineffective efforts designed around a discrete set of stove-piped compliance chores.[4]

The FSA's guidance document, issued during its consultation on CP11/12 last year, highlights some of these concerns. In it, the FSA finds that, *"although we identified some examples of good AML risk management, we found serious weaknesses common to many firms, particularly in relation to the approach to, and quality of, enhanced due diligence and monitoring of high-risk relationships; and the weighting given to AML risk as considered against profitability of accounts and reputational or regulatory risk."*[5] During the past year, the media has featured stories on several banks that have been cited and fined for deficient AML practices.

Furthermore, according to recent research by Gartner,[6] firms are also struggling to manage customer information more widely across products, relationships and geographies – this not only reduces customer service but also impedes efforts to tackle financial crime.

Financial institutions are caught between a rock and a hard place

The stakes are high and all institutions are under considerable additional pressure to cut back on costs. Fighting financial crime can be an especially burdensome obligation and it is not well-aligned with primary business objectives. This means that firms are possibly less motivated to do any more than be minimally compliant.

So what can organisations do to make their approach to financial crime more efficient and effective, and where should they start? How can they make the results more insightful to also improve overall customer service?

To tackle financial crime in a holistic and integrated manner, firms need first to pool their data, which has for too long been stored and processed independently. Wrapped around this integrated data set, firms also need to fuse capabilities for data management, data quality and analytics, as well as to set a clear strategy and appropriate mechanisms for governance, resourcing and reporting. To stimulate the market into action, the FSA recently launched its Core Financial Crime Programme (CFCP), which encourages firms to focus on the risks inherent in their overall business model rather than simply on the discrete set of systems and controls to manage those risks.[7] Tackling financial crime in this way creates discipline around risk management, with a defined risk strategy, risk appetite and a robust management framework.

Only by combining currently discrete approaches for AML, anti-bribery, counter-fraud and other types of financial crime can firms take advantage of the larger mosaic of data in which the web of crime appears. As firms begin to align their financial crime capabilities with other risk and regulatory activities, overall enterprise risk and performance management is improved.

Moreover, over time, this approach will set the stage for increased business value and improved service performance in a set of activities that the business has traditionally seen only as a cost and compliance centre.

Joining up the fight against financial crime

Where to start?

Financial crime approaches have become disconnected because many firms are essentially 'brown-field environments', in which activities have evolved as tactical responses to incremental changes in the external regulatory environment. Fractures have also occurred as organisations have grown and merged with others over time.

The data and technology used to tackle financial crime have thus often been duplicated across different parts of the organisation – in separate divisions responsible for retail, commercial and investment banking, for instance. This means that financial crime analysts are struggling to join the dots, and crimes are going undeterred, undetected and unchecked. In addition, operations have become costly and inefficient, and are now barely able to flex sufficiently to meet new regulatory requirements – a situation exacerbated by the multitude of legal and regulatory jurisdictions that many firms operate in and the essentially borderless nature of the crimes they are trying to defeat.

However, as crimes continue to increase in subtlety and sophistication – appearing to discrete intelligence systems as a set of unconnected and potentially normal account activities – the only way that firms can build an accurate intelligence picture is by connecting different pieces of data to form a kind of 'mosaic'. For example, a criminal who succeeds in committing a fraud is also a money launderer as soon as the proceeds of his crime enter the banking system; yet in traditional approaches the two crimes are not always linked or detected even though they are likely to have common, connecting elements. Similarly, alerts generated by AML transaction-monitoring systems may provide useful information to detect frauds – but only if the detection systems can join the dots. Overall, therefore, the analysis and interpretation of this mosaic is the key to detecting and, ultimately, preventing and deterring financial crime.

So firms seeking to take a more holistic approach to financial crime should focus on the vital role that data and analytics has to play in their operating model. It is only by centralising the current federated approaches to financial crime risk management that economies of scale and cross-domain activities can start to bear fruit.

In our experience, many firms want to adopt a more integrated approach to financial crime risk management but very few know where to start. Moreover, unless risk turns into crisis, firms often have no 'burning platform' that compels them to action. However, as firms are forced by renewed economic uncertainty to maintain their ruthless focus on cost reduction and efficiency, we believe that more and more will choose to fix the roof while the sun is shining.

Firms should approach integrated financial crime risk management using the following steps:

- **Assess where you are now** – the current state – for each crime area:
  - Do we understand what the cost of financial crime risk management is for our firm, and, if so, can we split it by cost type – considering people, technology and data (including the costs to obtain, store and analyse it)?
  - What processes are used to manage the data and control its quality?
  - How are teams organised and what are are their responsibilities?
  - How is performance measured and reported?
  - What steps are taken to ensure regulatory compliance?

- **Create a vision for where you would like to be** – the future state – which should include an assessment against your peer group in the market:
  - Are we actively seeking out opportunities to align areas of financial crime risk management?
  - Who has overall responsibility for managing and fighting financial crime in our firm?
  - Have we identified areas that can be more effectively aligned, for example, Know-Your-Customer (KYC) or Customer Due Diligence (CDD) data definition (including static and transaction), technology, analytics, investigations, policy and procedures, supporting standards, governance (including functional teams and committees), Management Information (MI), training development and delivery?
  - Do we think that the CDD information we have can give us greater competitive advantage or other commercial benefits. If so, how is this advantage to be gained?

We use the term analytics to describe a range of data-driven approaches that, when combined with deep business and sector knowledge, can highlight suspicious activity normally obscured by large data volumes or data stove-pipes.

- **Develop a roadmap to help you get from the current state to the future state** with a set of prioritised initiatives and projects, a high-level implementation plan and a business case:

  – How do we define 'effective' and 'efficient'?

- **Develop an outline of an integrated target operating model** that can be refined to fit the scale and precise business nature of the organisation:

  – How often do we review the effectiveness of the framework and look for further enhancements?

Delivering an insights-led operating model

The target operating model should be constructed around a central analytics 'hub' – the firm's engine room for financial crime risk management, which delivers high quality, actionable insights that can be used to detect, prevent and deter crime.

We use the term analytics to describe a range of data-driven approaches that, when combined with deep business and sector knowledge, can highlight suspicious activity normally obscured by large data volumes or data stove-pipes. The analysis draws on data sources from all financial crime activity in the firm – and potentially from external sources – to establish insights that provide a comprehensive and accurate assessment of risk, and is particularly powerful where the criminal activity is dispersed across several data sets.

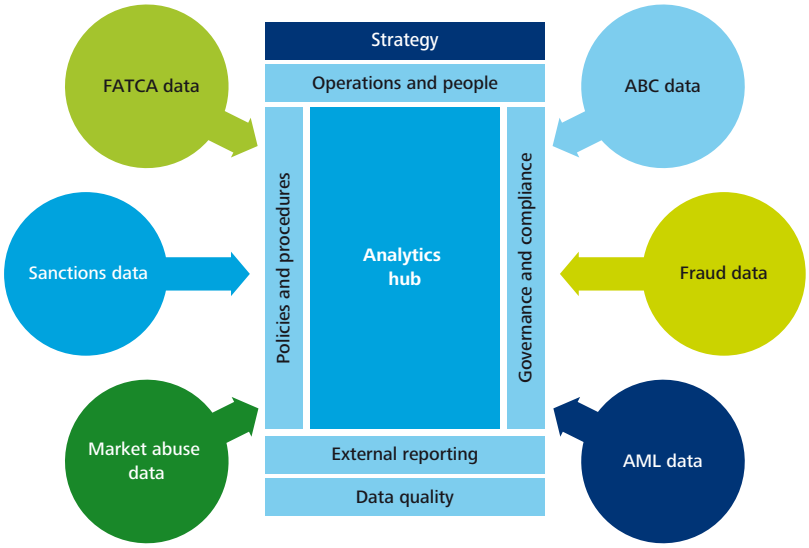
Examples of data that can be used are:

- transaction records;
- address;
- geospatial signals;
- personal identification;
- immigration;
- customs;
- tax;
- trade;
- payment;
- supply chain;
- human resources;
- payroll;
- open source /social media;
- internet clicks; and
- digital multimedia.

As links are made between people, account activity and transactions, a wide variety of techniques exist – applied alone or in combination – to reinforce and score links to help analysts join the dots and understand the overall risk.

As well as the data and technology for analysis, the operating model also needs to bring together elements of strategy, operations and people, policies and processes, governance and compliance, external reporting and data quality, which are necessary to deliver a unified risk management approach.

Figure 2. An analytics hub for integrated financial crime risk management



A centralised approach also allows managers to derive key performance indicators and timely and accurate Management Information, which can be used for essential benchmarking and reporting.

The operating model focuses on linking previously disconnected areas of financial crime activity, to explore the overlaps, synergies and linkages that exist between cross-firm data sets. Analysis can focus on historical data – to detect previously unnoticed crimes – or use data flowing into the firm to generate alerts that trigger more in-depth analysis. Ultimately, the data can be used to build models capable of estimating the probability of future crimes occurring, which means firms can become proactive rather than reactive, and thus reduce the potential for significant losses.

The other key areas of the operating model are:

- **Strategy** – focusing on areas including financial crime risk definition, identification and assessment; financial crime policy and framework.
- **Operations and people** – focusing on areas including structure, skills, process alignment and optimisation; operational effectiveness and efficiency; talent recruitment, development and training.
- **External reporting** – focusing on areas including reporting to the law enforcement authorities, regulatory bodies, industry bodies, and contact with the media.
- **Governance and compliance** – focusing on areas including compliance with and adherence to policies, assurance testing, periodic policy review, IT system governance, and incident and breach reporting.
- **Data quality** – focusing on areas including 'fitness for purpose' of data, data quality measures and monitoring, root-cause analysis of data quality issues and tools in use.

A centralised approach also allows managers to derive timely and accurate key performance indicators, which can be used for essential benchmarking and reporting.

Because it is based on facts rather than hypotheses, the analytics hub does not try to guess associations and therefore relies both on data volume and data quality. In some cases, data volume can provide a remedy for situations where data has been corrupted either accidentally or through systemic error, or where data fields simply have not been completed.

The use of analytics is often compared metaphorically to 'finding the needle in the haystack'; the unified approach to financial crime risk management is effective not only because the analytics ultimately finds more 'needles' but because it also very effectively characterises and removes the 'hay', leading to greater efficiency as well as a better understanding of the financial crime situation overall.

The analytics hub in practice

Overcoming common challenges

There are two primary challenges with obtaining the data required for meaningful intelligence. First, identifying and extracting relevant data is complicated because it typically resides in multiple locations and is 'owned' by many different people. Second, the quality of this data is typically poor: not just missing or inaccurate data, but data that is also not 'fit' for its intended purpose.

Both of these challenges can be overcome using the analytics hub at the centre of the target operating model, but a number of other common challenges exist:

Devolved executive responsibility

- ***Challenge*** – in many firms, each type of financial crime is the responsibility of a different executive. This tends to drive a wedge between approaches to tackling financial crime because these individuals want to retain sovereign control and oversight of their area. The situation is made worse because significant criminal and civil fines and penalties would single them out should they fail.

- ***Response*** – use the target operating model to define a clear strategy and organisational approach that has clearly defined roles and responsibilities for financial crime risk management. Ensure that compliance procedures and external reporting requirements are built into overall governance. Moving to a centralised model should ensure that subsequent processes for risk management and compliance are simpler and more efficient.

Organisational barriers

- ***Challenge*** – often departments will deliver their work in line with the classic hierarchical organisational structures inherent in many financial institutions. Standard reporting lines and entrenched approaches do not allow them to adopt a more collaborative and proactive working style with other areas of the organisation. Individual departments are also often responsible for their own technology and data, and these territorial approaches undermine and limit the effectiveness of cross-organisation risk management.

- ***Response*** – although many businesses are resistant to organisational and business change, firms need to grasp the nettle with their data and drive through the changes required to adopt the target operating model. When strategic goals are thus aligned, collaboration becomes much more effective and multi-disciplinary teams are then formed for each step in the data capture, storage, management, analysis and reporting process.

'Bolt-on' approaches to meeting new regulations

- ***Challenge*** – often, firms address new or amended regulatory requirements by 'bolting on' new teams, processes, procedures, MI or technology and data infrastructures. This may be done, at least initially, as a 'quick-fix' to meet a specific regulatory deadline or because the existing infrastructure is simply too difficult to change. In the longer term, though, the results are suboptimal and can hamper efforts to improve the overall efficiency of financial crime risk management.

- ***Response*** – with a unified approach to financial crime risk management, firms are more easily able to define a single roadmap to improve analysis maturity and capability that is aligned with planned changes in legislation or regulation. Firms should also think about deploying an analytics 'sandbox', which allows teams to experiment with new data and new technologies without compromising the efficiency and effectiveness of the operational analytics hub. Sandboxes provide a way of assessing new techniques in advance of regulatory changes so that the target operating model – and the data and analytics in particular – can be optimised in time to meet any deadlines.

More pressing priorities

- ***Challenge*** – given the harsh realities of today's operating environment, it should come as no surprise that board members have been focusing on the sources of acute stress on their firms: renewed economic uncertainty, proposed banking sector reform and various legacies of customer mistrust following the credit crisis of 2008 and mis-selling of payment protection insurance, for example. As a consequence, and despite regulatory pressure ratcheting upwards, financial crime risk management has dropped down the priority list.

- ***Response*** – the target operating model provides firms with a streamlined approach to financial crime risk management, which means that regulatory obligations can be met more efficiently as well as more effectively. The insights provided by the analytics hub also deliver intelligence to support more positive engagements with law-abiding customers. The unified approach, therefore, could not only reduce losses from financial crime but also mitigate risks caused by poor knowledge of customers – the sorts of risks that contributed to the current climate of stress.

Efforts to tackle financial crime thus need to be streamlined into something smarter and more agile. Focusing on managing the overall business risk from financial crime, rather than on attempts to strengthen the set of individual systems and controls, will help firms to overcome these challenges. And there is considerable upside to be had through amalgamating the various sources of data that are currently generated in financial crime silos. For instance:

- analysts can relate the detection of potential fraud to the increased risk of money laundering;

- law-abiding customers will enjoy an improved experience because better quality alerts will lead to fewer 'false alarms';

- the firm can develop a more accurate picture of the firm-wide costs of tackling financial crime and complying with relevant regulations;

- the firm can achieve cost savings by reducing the number of discrete teams tackling financial crime;

- data managers can achieve a better understanding of the quality of data used for financial crime reporting, which will enable root-cause analysis to be performed to ensure data quality is optimised in the future; and

- the firm will benefit from greater clarity on data ownership, which will improve accountability for data quality across the business.

What does 'good' look like?

There are two examples that illustrate how the target operating model can improve upon current approaches to financial crime risk management:

- Customer Due-Diligence (CDD) data; and

- people management and development.

Customer Due-Diligence (CDD) data, also known as Know-Your-Customer (KYC) data, is gathered for a number of reasons, which include financial crime risk management – such as AML screening and monitoring, CTF (Countering Terrorist Financing) monitoring, sanctions screening, FATCA compliance, ABC monitoring and fraud monitoring. Under typical current approaches, each area would request a different dataset and firms typically collect the (often overlapping) information in several different formats and on different systems. CDD data is also gathered for credit risk assessment, for client classification and suitability (under MiFID, The Markets in Financial Instruments Directive), and for a range of other business purposes, for example marketing or to cross-sell products.

By defining and populating a complete customer master dataset in one location, firms can use this single source of information to tackle the various types of financial crime and also enhance customer insight. The key here is to invest time in defining the dataset and recording it on a system with agreed protocols for ease of use and maintenance.

Having a more integrated and holistic understanding of customers can be exploited for the benefit of other business units and can deliver considerable commercial advantage. It also provides a consistent view of client information, which can be updated centrally.

Efficient collection of data eliminates the duplication of effort that typically causes reconciliation and inconsistency issues, as well as the costly maintenance of several systems.

Furthermore, financial crime risk management is a labour-intensive activity. People are needed for customer on-boarding, central compliance and oversight, as well as large monitoring, screening and investigation teams. Some of the roles performed can be repetitive and monotonous, which can lead to high staff turnover and general inefficiency as productivity drops.

Firms can align and integrate resource requirements across all areas of financial crime thereby creating opportunities for team members to work on different activities and making the roles more interesting and appealing.

The integration and alignment of people requirements for the various types of financial crime improves staff retention and productivity as the role becomes more varied and interesting. The integrated and collaborative nature of financial crime risk management creates a multi-skilled workforce, which eliminates single points of failure and helps firms manage skill shortfalls.

The integration and alignment of people requirements for the various types of financial crime improves staff retention and productivity as the role becomes more varied and interesting.

Getting the right outcome

Avoid the path of minimal compliance

In today's highly complex and volatile financial markets, it is harder than ever for financial institutions to detect and prevent financial crime. Yet continually evolving regulations relating to financial crime and customer due-diligence are compelling firms to improve.
With a legacy of disparate approaches to contend with and increasing pressure on costs, firms could easily choose the path of minimal compliance. Before they take this line, though, they should consider whether an integrated approach, centred on bringing their data and analytics together, would help them to improve the quality of their financial crime intelligence while simultaneously reducing costs. Rather than continuing to pump time and money into a patchwork of activities to tackle financial crime, firms should start with their data. They should assess their cross-domain capabilities and subsequently develop a target operating model that aligns strategy, people, process, technology and data capabilities.

Without such an integrated approach, firms will continue to invest in activities that simply do not provide the flexibility to keep up with changes in the regulatory landscape or the increasing sophistication and subtlety of criminals. With no way of joining the dots in their data, the effectiveness of risk management will eventually degrade. Firms that fail to improve or at least maintain effective measures against financial crime are likely to suffer greater financial loss and reputational harm, and firms and their employees will be left more vulnerable to punitive action by the regulators.

Faced with these harsh realities, firms need to focus on their data to ensure that they improve overall risk management and ultimately deliver the desired business outcomes.

An integrated approach improves customer service, too

An integrated approach to data also enables firms to seek out additional synergies between financial crime intelligence and customer intelligence, thereby creating opportunities to improve customer services and add more business value.

For example, customer data that is obtained for KYC purposes, such as source of funds or source of wealth, could also be used to deliver more tailored product marketing. Similarly, customer profiles created for AML transaction monitoring purposes are just as valuable for segmenting customers for marketing. The synergies run both ways: the insight gained from the day-to-day processing of credit card transactions is also likely to help financial crime teams get a better understanding of customers' money laundering risk profiles.

With a little creative thinking and an integrated approach, financial institutions can improve their risk management and customer service. There is really only one practical way forward.

References

1 http://www.fsa.gov.uk/about/what/financial_crime

2 Speech by Callum McCarthy, Chairman, FSA, 15 November 2005

3 CP11/12 Guidance for firms (http://www.fsa.gov.uk/pubs/cp/cp11_12.pdf)

4 JMLSG 2007 Guidance, 20 December 2011, (http://www.jmlsg.org.uk/news/further-amendments-to-2007-guidance-20-december-2011}

5 CP11/12, FSA Guide for consultation (June 2011 http://www.fsa.gov.uk/library/policy/cp/2011/11_12.shtml)

6 Gartner research report, Leverage AML Technology to Create Business Value Published: 26 April 2011

7 http://www.fsa.gov.uk/pubs/newsletters/fc_newsletter15.pdf

Contacts

Tom Scampion
Partner
Enterprise Risk Services
+44 (0) 20 7007 2828
tscampion@deloitte.co.uk

Michael Jones
Director
Enterprise Risk Services
+44 (0) 20 7303 8673
michajones@deloitte.co.uk

Harvey Lewis
Research Director
Deloitte Insights
+44 (0) 20 7303 6805
harveylewis@deloitte.co.uk

www.deloitte.co.uk/analytics

www.deloitte.co.uk/analytics

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 18030A

Member of Deloitte Touche Tohmatsu Limited