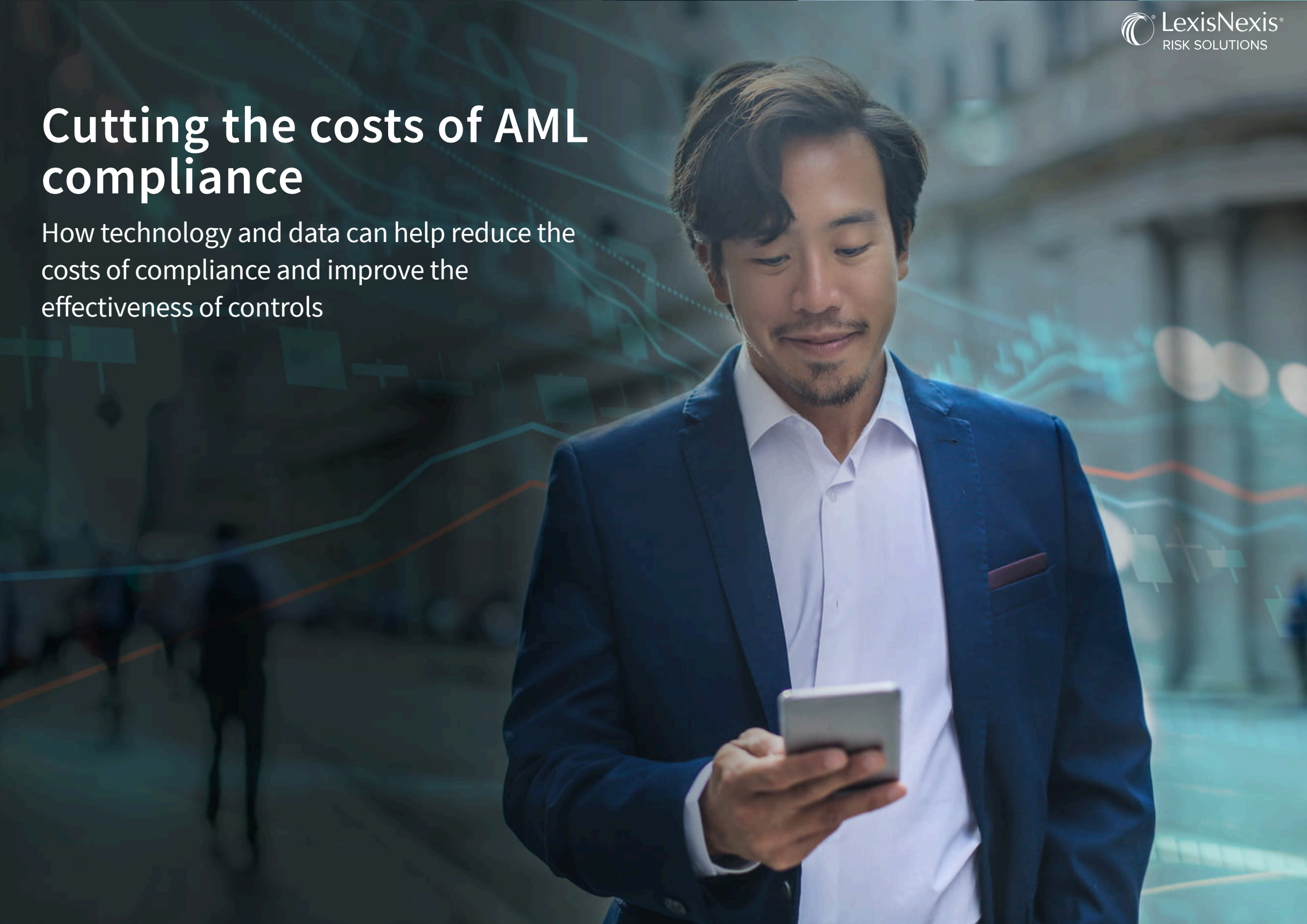
LexisNexis®
RISK SOLUTIONS

Cutting the costs of AML compliance

How technology and data can help reduce the costs of compliance and improve the effectiveness of controls

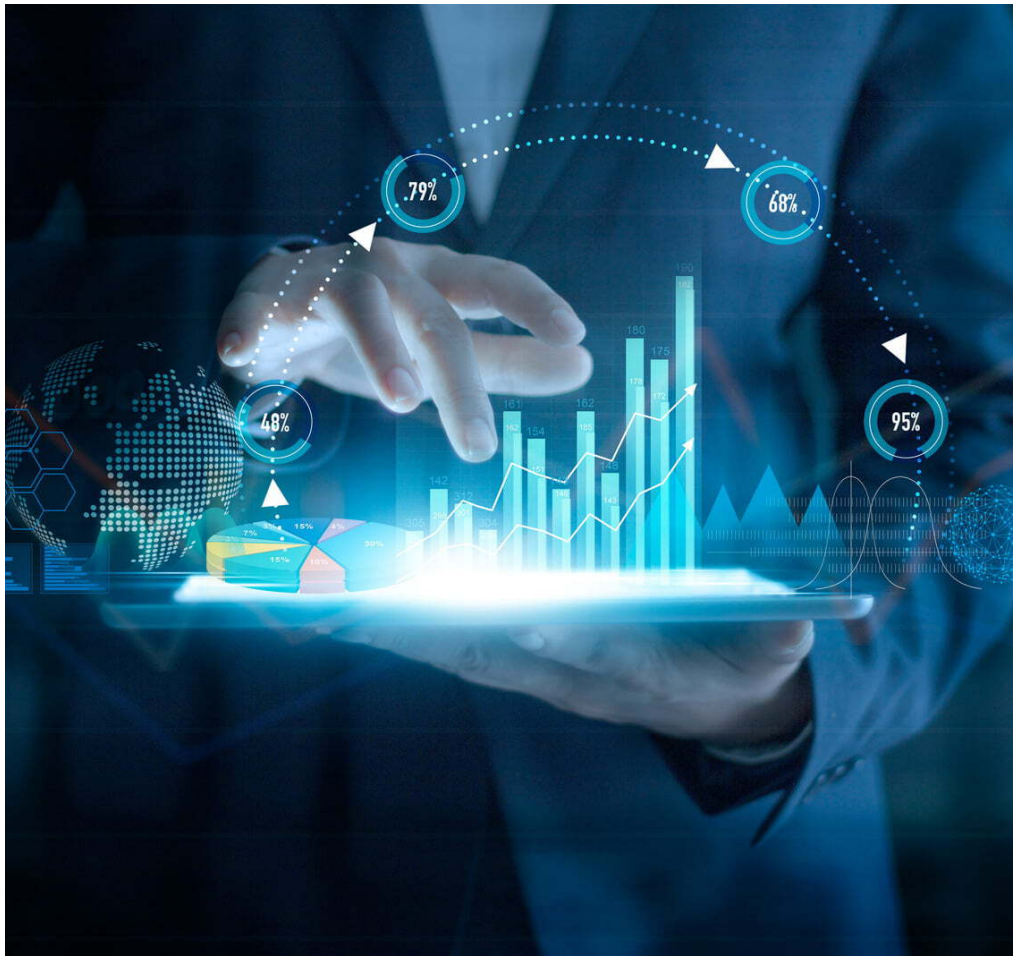


LexisNexis®
RISK SOLUTIONS

Executive Summary



Summary of Findings



UK AML compliance costs are high and set to grow at an increasing pace. Increased AML regulations, more so than criminal threats, are driving up costs. Interpreting complex legislation is time-consuming and costly. Growth in volumes of AML activity contributes to higher costs. In many cases, AML processes are costly and time-consuming. Fear of the regulator stands in the way of progress. A culture of over-cautiousness leads to over-reporting of suspicious activity, resulting in higher volumes of work. AML compliance spend is heavily skewed towards people-related costs, rather than technology. An over reliance on people renders firms vulnerable to staff attrition and human error. Is it time to redress the balance and shift compliance spend towards technology rather than people? Data and technology are already helping to reduce time and costs, but could do much more.

This report draws on our research with Oxford Economics[1]. We spoke to over 300 of the UK's leading financial institutions and conducted in depth interviews to determine an accurate figure for the cost of compliance operations for UK firms, analyse trends in AML costs, and explore potential factors influencing cost behaviour. Unless otherwise referenced, any statistics in this report are taken from this research.

LexisNexis®
RISK SOLUTIONS

The rising cost of AML compliance in the UK



UK AML compliance costs are high and set to grow at an increasing pace

The annual cost of anti-money laundering (AML) compliance for financial institutions in the UK is estimated to be a huge £28.7 billion, with costs expected to grow more steeply in the next two years, reaching over £30bn by 2023.

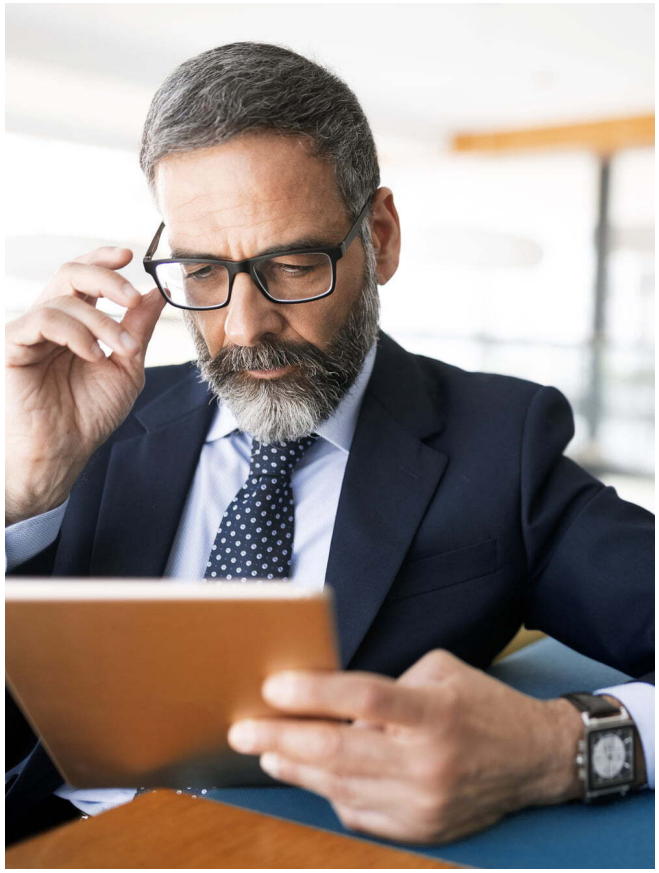
This seems very high when you consider:

- The National Crime Agency estimates the total annual cost of serious organised crime to the UK economy to be around £37 billion[2].
- The entire UK annual defence budget for the year ending March 2021 was £53.3 billion[3].

On the other hand, the cost may be more justified when you consider the size of the money laundering problem facing UK plc, which a **financial crime intelligence leader of one of the top tier UK banks** describes as 'absolutely massive': *"If you look at some of the key threats that we're seeing as a bank, and then if you multiply that by the number of banks that are out there and all the other players that play as part of the process of executing transactions that can be susceptible to money laundering, I think we've got a considerable problem on our hands."*

Firms in the survey reported an average AML compliance cost of £186.5m per annum. For larger institutions average costs are closer to £300m, or more. In the past three years, firms reported that financial crime compliance costs have increased broadly in line with business inflation (up by 5.4%), however future cost inflation for AML and CFT compliance is expected to be more severe over the next three years, at nearly 10%.

Reported costs correlate strongly with firm size: despite lower absolute costs, evidence shows that AML compliance costs are more burdensome for smaller organisations, due to a lack of economies of scale[4].



Regulations, more so than criminal threats, are driving up costs

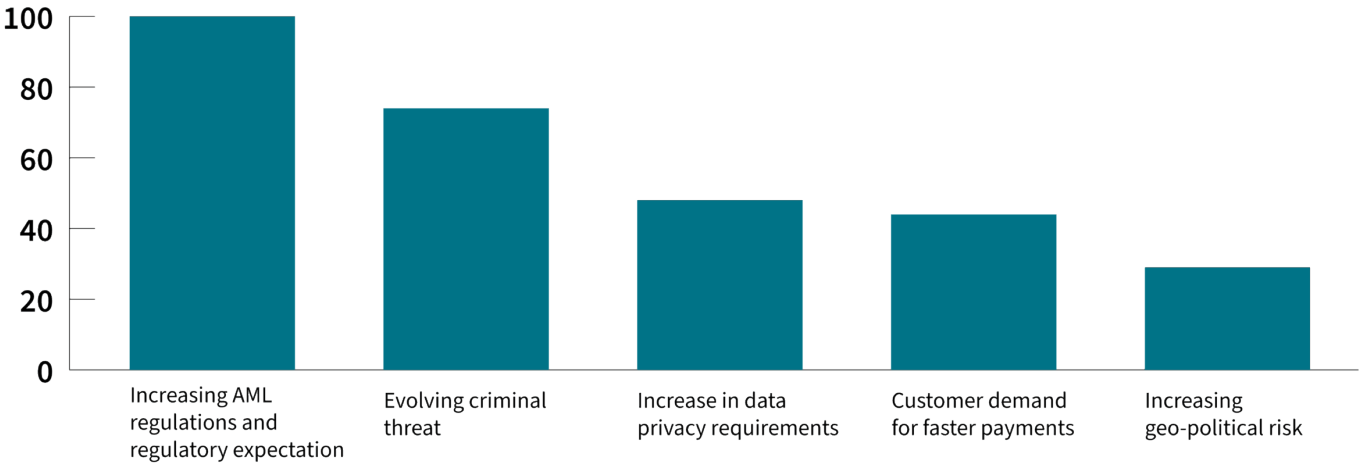
It might be assumed that evolving criminal threats and risk profiles would be the biggest external factor in driving up financial crime compliance costs, as criminals constantly seek to outpace the systems and controls that are put in place to stop them.

However, a significantly bigger driver of costs appears to be the regulatory expectations themselves, and the fear of being fined for non-compliance. – see Fig 1.

Firms report that the increasing volume and complexity of AML regulations have been the most significant external driver of cost: In 2020, UK money laundering regulations integrated the requirements of the 5th Money Laundering Directive (5MLD) and UK firms estimate that it will cost them, on average, around three quarters of a million pounds[5] to implement.

Perceived importance of external drivers of increased compliance costs*

Index value, highest perceived risk = 100



*Only firms which said their costs had increased vs three years ago

Fig. 1

Turning the super-tanker: The impact of regulation



For many firms, the cost of complying with money laundering regulations is wholly disproportionate to their size and level of risk.

One **MLRO of a mid-sized building society** admitted his organisation is spending £200-£250k per annum on screening alone (systems and staff), to comply with money laundering regulations, despite the nature of their business and perceived risk of money laundering being very low.

"The regulators don't necessarily understand the granular impact of some of the changes they're making", says **Group Head of Financial Crime for a UK specialist lending bank.**

They cite the example of the UK sanctions regime that came into force at the start of 2021. The new regime didn't constitute a massive change in terms of what was actually on the sanctions list, as most were already on the UN or the EU list. However, there were a number of administrative changes made that didn't constitute any change to the level of risk or restriction, but that nevertheless had a big impact on referral rates, resulting in a huge spike in alerts at New Year for UK compliance teams to deal with.

Interpreting complex legislation is time-consuming & costly

The money laundering directives themselves are really complex, so most firms look to the Joint Money Laundering Steering Group (JMLSG) for guidance. That said, the JMLSG interpretation tends not to be issued until some weeks after the legislation is introduced. As a result, directives that involve major changes for a lot of organisations, as was the case with the 4th EU Anti-Money Laundering Directive (4MLD), can be a real challenge for organisations to implement and the cost of covering that is quite significant.

Group Head of Financial Crime for a UK specialist lending bank explains: *"Some of these changes are like turning a super-tanker, particularly for the larger organisations. Processes are embedded, so the sooner you can get the guidance out, the better."*



Brexit is likely to result in more regulation, not less



Financial institutions don't expect the UK's exit from the European Union to alleviate AML compliance cost pressures. On the contrary, they anticipate it will actually result in more regulation rather than less. So, if anything, the UK's regulated sectors expect AML compliance costs to rise more steeply in the coming years, as a result of leaving the EU.

As one MLRO from a mid-sized bank puts it: *"Costs are rising because the asks are increasing. Brexit will bring increased complexity and lack of clarity because we have EU sanctions, US sanctions and now we have UK sanctions too, so it is getting too complicated and, therefore, more difficult to implement."*

LexisNexis®
RISK SOLUTIONS

The impact of excessive regulation



Excessive regulation stands in the way of progress

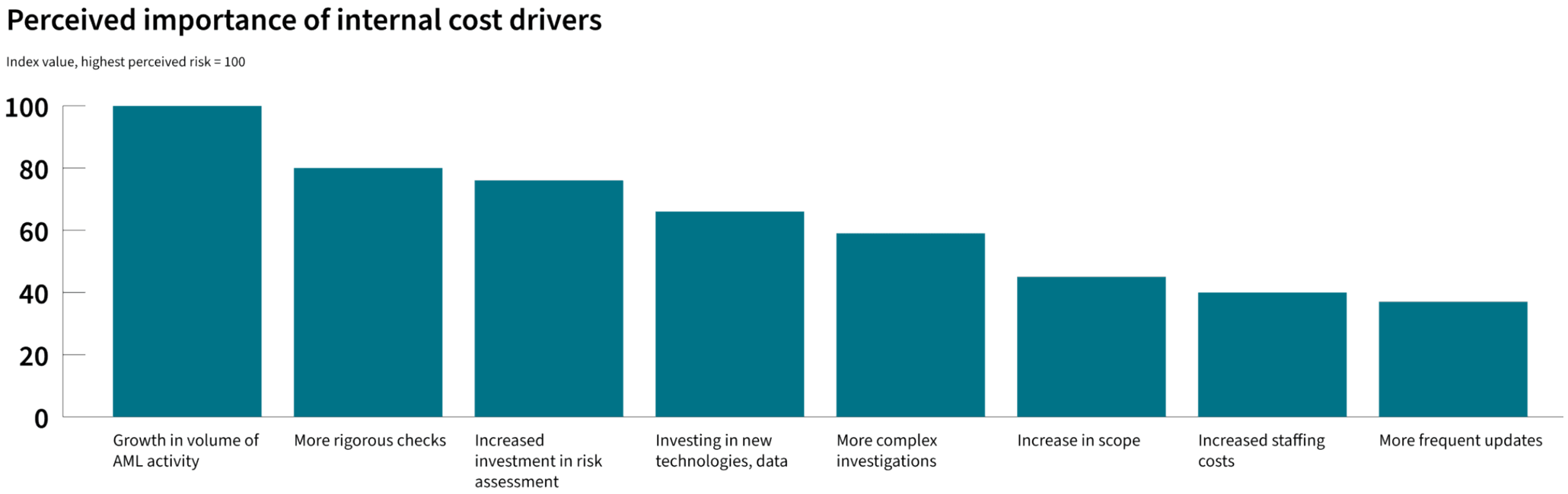
The danger is that excessive regulation creates an environment where financial institutions become too focused on complying with the laws of the land and managing the systems and controls to do so, to the detriment of spending more time considering how to fight financial crime more effectively.

Financial crime compliance leaders need to balance the need to comply with regulation, with the very real need to build sustainable and effective systems and controls and future-proof them. Many lack the bandwidth to do both at the same time. Thinking of new and better ways to combat financial crime is exciting, but breaking protocol and encouraging change demands a lot of effort and respondents report a fear of 'dropping something inadvertently' with regards to regulation, and having to face the consequences. This acts as a deterrent to innovation.



Growth in volumes of AML activity contributes to higher costs

Growth in the volume of AML activity is perceived to be the most important internal driver of total AML costs. – Fig 2.



Source: Oxford Economics

Fig. 2

A senior compliance professional at a leading currency exchange provider told us they expect the compliance burden to continue to increase as a result of media coverage around money laundering and COVID-related scams: *"Whenever a scam hits and wherever it's extensively covered in the media, there's an inevitable reaction from legislators, which unfortunately, adds burden on the compliance function."*

Steve Payne of Vitality Group also attributes the increase in activity to the fact that financial crime compliance has moved up the boardroom agenda in recent years. He talks of, *"a cultural realisation of the importance of compliance"*, for the Insurance industry: *"In the last two to three years, financial crime has very much gone up the agenda. It's a general realisation that it's a major topic and it's a hot topic with both the regulator and law enforcement."*

Graeme Morrison, Head of Financial Crime at Ardonagh Group agrees: *"I would say the volume of compliance activity is increasing, because I think the business now understands the value of it. The business sees compliance as a partner in doing the right thing and in some ways, being a bit of the conscience of the organisation. And it helps management make the right decisions."*



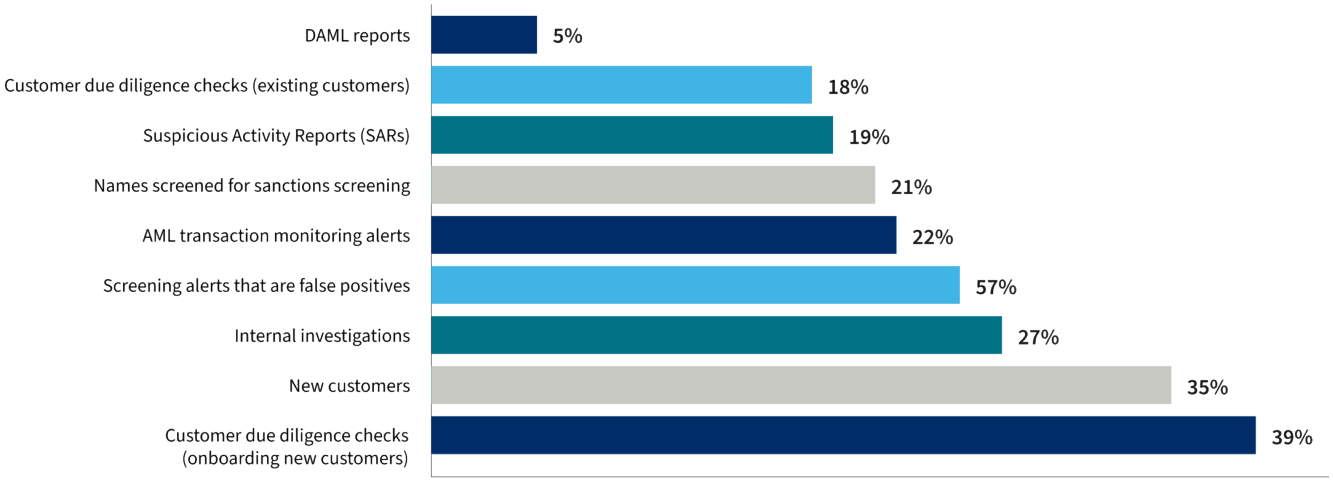
Business growth appears to be the primary driver of additional compliance activities

The most important catalyst of increased AML compliance activity over the past three years appears to be associated with business growth - taking on new customers and running customer due diligence checks for them. Investigative and alert-related activities were next most cited, with back-end processes, such as compliance activity reporting, typically the least likely to have increased, versus three years ago.

Fig 2b shows the net balance of respondents reporting increased volumes of AML compliance activity over the past three years, less those who reported a decrease. All activities showed a net positive balance, but there was significant variation across categories.

Net balance of respondents responding that AML compliance volume had increased vs three years ago

Share of respondents



Source: Oxford Economics

Fig. 2b

Increased criminal activity during the pandemic is causing spikes in suspicious activity and alerts

The global pandemic has created a list of challenges for AML compliance staff, topped by increased criminal activity, with almost 50% of institutions recording spikes in alerts and possible suspicious activity – see Fig 2c. Almost half of respondents (43%) also cited interruptions to their compliance monitoring capabilities, as a major challenge, no doubt in part fuelled by the lockdown-induced shift to home-working and in some cases, the need to furlough staff.

What AML compliance challenges (if any) has your organisation experienced during the COVID-19 pandemic and the remote working period?

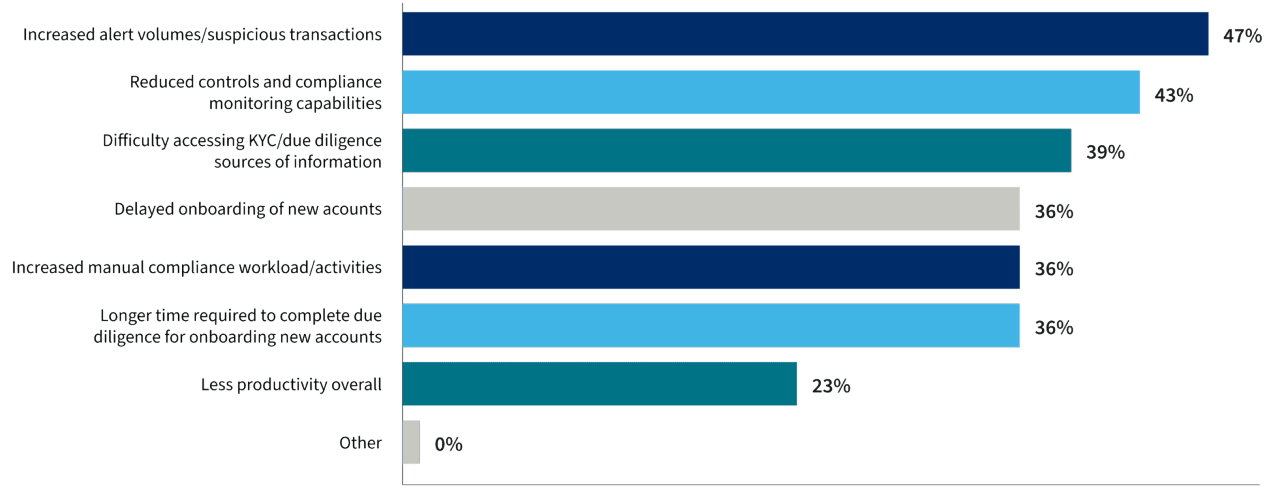


Fig. 2c



LexisNexis®
RISK SOLUTIONS

Breaking down the cost and time spent on AML processes

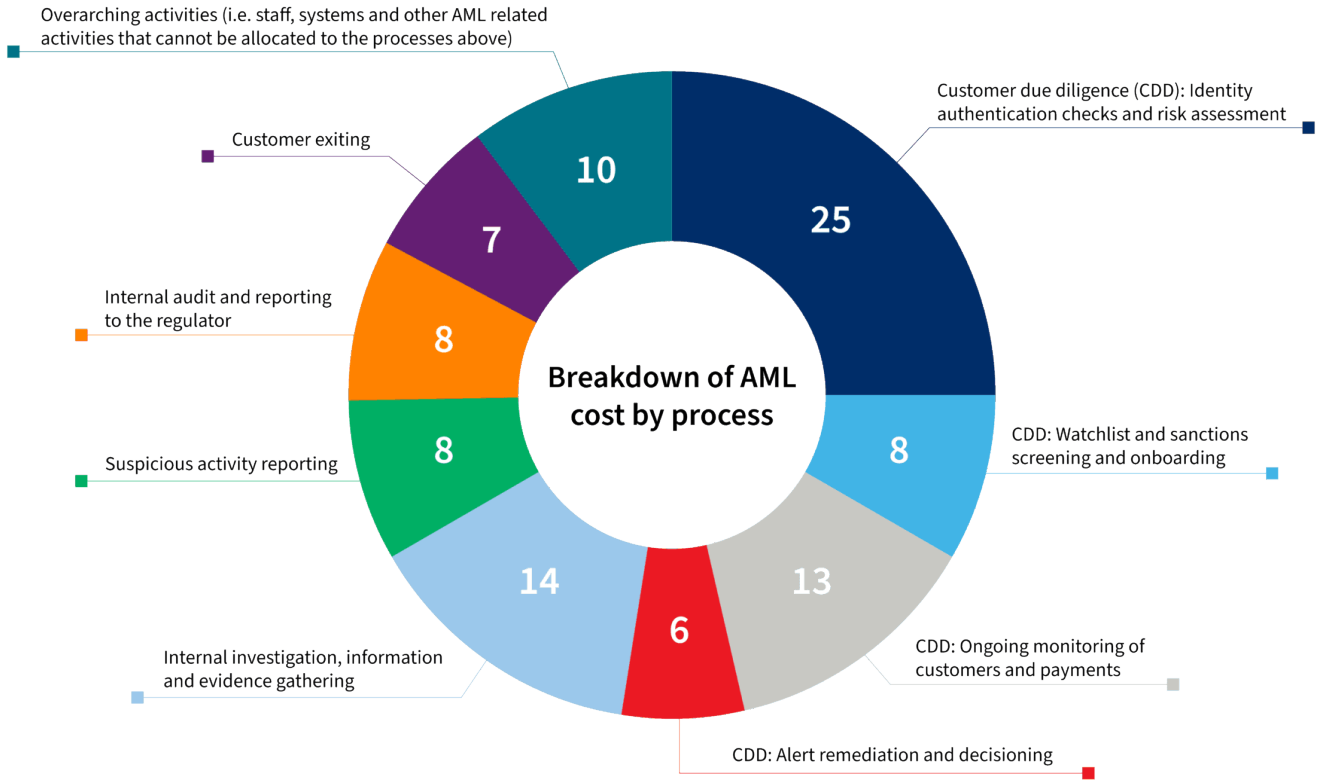
In many cases, AML processes are costly and time consuming

Respondents cited a number of issues that hamper the efficiency and effectiveness of their AML compliance processes, including data quality, system failures, gaps in IT infrastructure, ineffective internal tools and outdated technologies.

We asked firms to estimate how their financial crime compliance costs are split between the various processes. There was little discrepancy between the percentage share of costs and the percentage share of staff time reported for each of the processes.

Over half of AML compliance budgets are spent on customer due diligence

Together, customer due diligence (CDD) processes and investigations account for two thirds of total AML and CFT compliance time and cost. CDD was by far the most costly and time-consuming process in our sample, accounting for 53% of overall AML compliance costs – see Fig 3.



Source: Oxford Economics

Fig. 3

Greater emphasis on ‘Know Your Customer’

It’s no surprise that firms are spending a lot of time on customer due diligence. The 4th EU Anti-Money Laundering Directive, integrated by the UK into the 2017 Money Laundering Regulations, mandated a number of changes that drove this greater emphasis on CDD.It required obliged entities to provide evidence that they have undertaken appropriate levels of CDD and to take steps to understand beneficial owners.

It also widened the definition of politically exposed persons (PEPs) and mandated other changes in relation to record keeping and reducing the limits on transaction values to trigger CDD. The 5th EU Money Laundering Directive, which was integrated into UK regulations in January 2020, further tightened these rules and also recognised the growing use of electronic identity verification (EIV), permitting obliged entities to conduct EIV with a trust service. This, in turn, triggered a need for regulated firms to review their technological infrastructure to support digital identification in onboarding, which for many, was no small task.

Our survey shows that more rigorous checks and increased investment in risk assessment were among the top three internal drivers of increased cost in AML compliance – see Fig 2. In fact, half of CDD costs (and a quarter of total financial crime compliance costs) relate to identity authentication checks and risk assessments.



Perceived importance of internal cost drivers

Index value, highest perceived risk = 100



Source: Oxford Economics

Fig. 2

Balancing the need for a frictionless customer journey with the need for robust customer due diligence

Compliance teams are facing mounting pressure to design processes that work around the customer journey and balance the need for speed and convenience with the requirement for effective compliance.



"One of the buzz phrases now is 'customer journey', but there will always come a point where you've got to be careful that the customer journey is not so streamlined and so quick that you miss your own responsibilities within the regulatory and legislative framework. My challenge is making sure that my mandate gets fulfilled, as well as meeting the commercial expectations of the firm, and keeping the customer, or the applicant, happy."

– Steve Payne, Group Head of Financial Crime and MLRO, Vitality Group

Customer expectations are changing. Increasingly, customers are now expecting a response almost instantaneously and are far less prepared to wait. They also want the convenience of being able to apply whenever it suits them, and more likely than not, online or by mobile. Offering customers faster and more convenient onboarding represents a challenge for compliance teams who need to ensure their identity checks and risk assessments are equally robust and secure, regardless of how the customer chooses to apply. Since the start of the pandemic, the boom in remote Know Your Customer (KYC) and identity verification needs has put significant pressure on businesses to carry out quick and effective identity checks that negate the need for customers to send physical identity documents by post. The technology required to facilitate this is already ubiquitous – customers can use their phones to scan the chip on their passport and submit a selfie. The company then simply compares the two. There is now mounting commercial pressure on all businesses to adopt this technology to meet customer demand.

However, as Chris Leatherland, Head of Financial Crime at NewDay explains: *"The problem is that biometrics, at their very core, depending upon how verified or matched, don't necessarily currently meet the legal requirement in the Money Laundering Regulations and the Guidance Notes. So, despite the fact we could potentially do it, there isn't currently the necessary regulatory aircover to say you're allowed to do it."*

As a result, many firms are reticent to go through the expense and process of embracing some of these newer and more efficient technologies, for fear of regulatory reprimand. Instead, they appear to be watching and waiting for the regulator to make the next move.

Screening & ongoing monitoring make up a fifth of overall AML compliance spend

Firms are required to verify the identities of new and returning customers and screen for global sanctions and enforcements, PEPs and for instances of higher risk adverse media, which may pose financial, regulatory and reputational risk to the business. Where firms have millions, or even billions of customer accounts, this can be a real challenge. The frequency of screening depends on the firm's chosen risk-based approach, however, given the 24-hour news cycle and ever-shifting sands of global politics, many firms screen their entire customer base, daily.

Added to this, the landscape of global threats is constantly changing, making it difficult and time consuming to compile real-time global intelligence in house. Doing so also inevitably slows workflows, increasing the cost of doing business and taking the focus off core business activities. It's no surprise therefore that a further fifth (22%) of overall financial crime compliance costs relate to watchlist and sanctions screening at onboarding, as well as the ongoing monitoring of customers and payments.

Graeme Morrison of Ardonagh Group paints a picture of his organisation's regular and thorough customer due diligence controls:

"We have metrics and controls in place around the onboarding. We have automated screening, and we screen all clients, six days a week. We have real-time screening for where we're making payments to individuals who are not part of that automated screening. We screen all staff, we screen all suppliers, we screen all incoming businesses."



Alert remediation, investigations & evidence gathering comprise a further fifth of AML compliance spend

The triage processes deployed to effectively risk assess and segment customers for AML screening are coming under increasing scrutiny. Firms are reportedly taking more than 20 hours to remediate even standard risk customers – which in 90% of cases, turn out to be false positives. This is in line with the findings of our research from three years ago, which showed a typical KYC remediation case took on average 18 hours and 3.7 staff members to complete, with a typical sanction remediation case taking a similar time, on average, albeit with fewer staff.

For banks, the average processing times for both KYC and sanctions remediation are closer to 24 hours - nearly double the time taken by investment firms (13 hours)[6]. According to one MLRO at a mid-sized building society, current screening generates about 100 alerts per day of which around 10 percent need escalation or investigation. Of these, very few actually turn out to be the result of financial crime. False positives are one of the biggest operational issues that financial crime compliance teams face and constitute some 95 percent or more of the investigations they have to check. Despite their team's ability to identify false positives within a few minutes, those that do require escalation often take all day to remediate and in the bulk of cases, these also turn out to be false positives.

There are a variety of underlying factors which drive inefficiencies in remediation processes, including disparate data systems and the lack of a single view of customer risk. Incomplete or out of date data impacts the number of alerts that financial crime teams have to deal with, as well as creating delays for ongoing screening if customer data is missing or inaccurate. It also impacts customer experience, both through delays and the intrusion of being contacted to re-verify their details. To make matters worse, this is not necessarily an area over which compliance teams have much control, as responsibility for customer data usually sits with another department.



Data quality is quickly moving up the agenda, with artificial intelligence leading the revolution

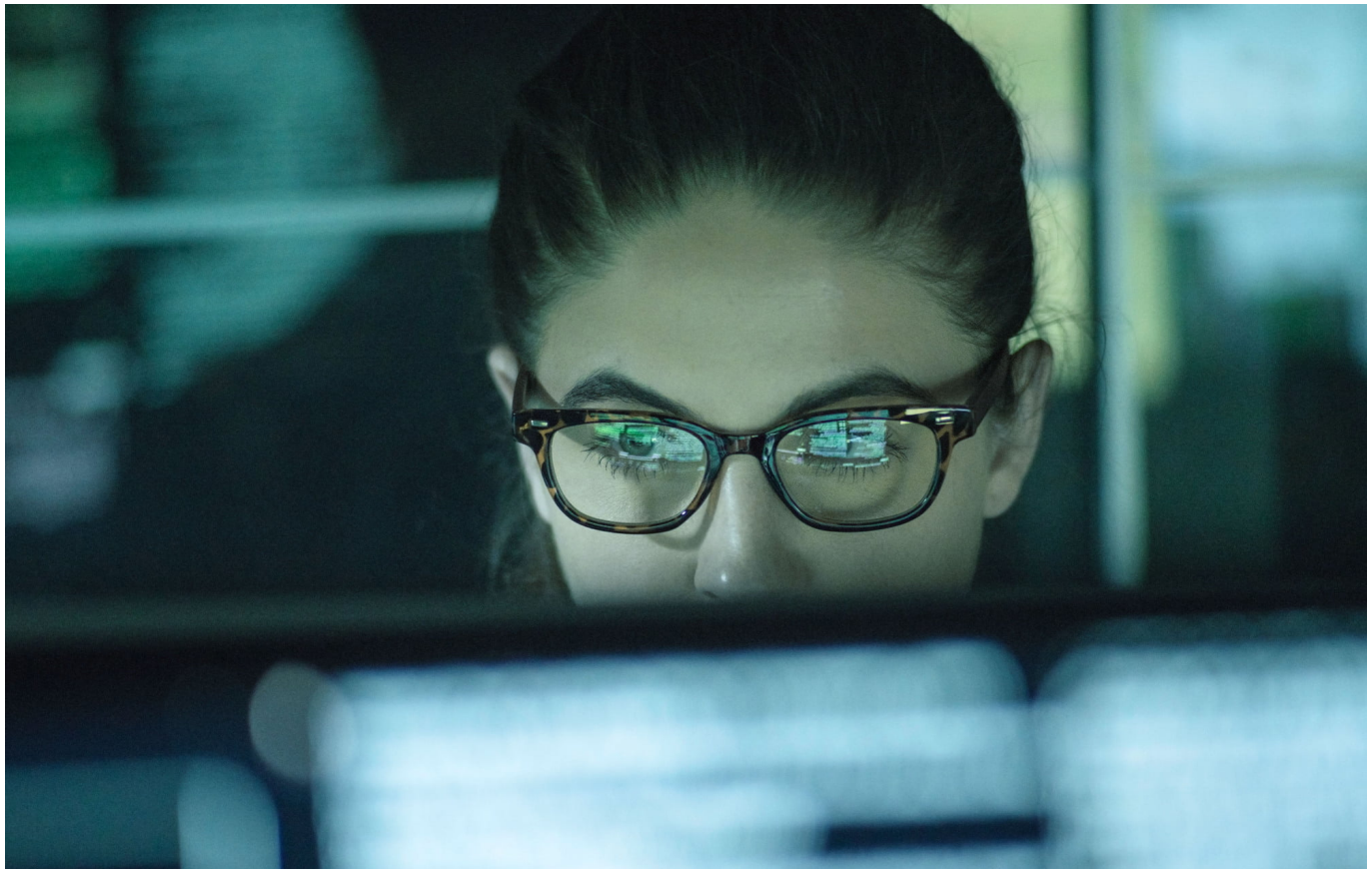
Banks need to do things more efficiently and cost effectively. There is a big drive to understand customers better, driven partly by the emergence of Open Banking and partly through competitive pressures. The success of all of which is predicated on the quality of data. Having clean data, in the right format, which is easily accessible and retrievable is becoming increasingly fundamental. However, many of the bigger financial institutions and particularly those that are part of big groups, struggle to achieve a single view of the customer, due to multiple brands and separate business areas with different systems and interfaces.

Implementing an effective risk-based approach to AML regulatory compliance processes could be made drastically easier simply by establishing a rich, accurate and holistic view of customers, through a robust customer data management system.

Addressing this could have an exponentially positive effect on a firm's ability to effectively risk-assess customers. Not only that, but a knock-on effect would also be a reduction in the entire down-stream compliance time and cost commitment, thereby reducing the mammoth resources currently being lost to remediation and needless investigations and enable compliance teams to focus on the real issue of managing financial crime risk more effectively.



Stricter requirements of 5MLD are also adding to firms' AML compliance burden



Beyond remediation, the 5th EU Anti-Money Laundering Directive also tightened the rules around EDD, extending the definitions of what constitutes ‘higher risk’ and requires EDD investigations, as well as extending the types of information needed to be gathered for CDD checks.

Many firms rely on their own resources to conduct EDD checks, yet without the correct tools and support, this can be time consuming and leave them exposed to unseen risk.

A culture of over-cautiousness leads to over-reporting of suspicious activity, resulting in higher volumes of work

Suspicious activity reports (SARs), widely mooted as being a heavily time-consuming activity, in reality take up less than 10% of AML compliance professionals' time, according to our study. The issue here is perhaps, not resource, but a perceived lack of a return on investment. As most AML compliance professionals will attest to, in the vast majority of cases, businesses won't receive any feedback on submitted SARs or DAMLs and get no sense as to whether it was time well spent.

Another issue with the SARs regime is the propensity for 'defensive reporting,' – firms intentionally over-report to err on the side of caution, taking solace in the fact that they've discharged their legal obligation, even after they've facilitated the transaction and taken their fee. The resulting glut of reports inevitably overwhelms the system.

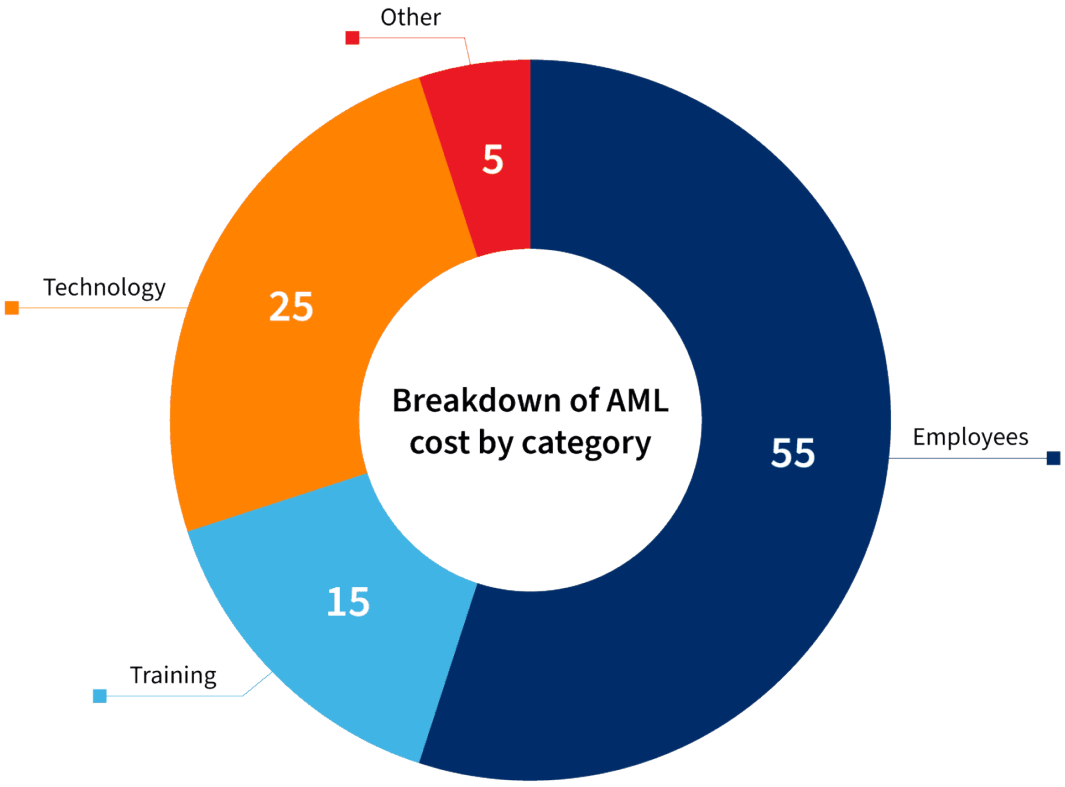



LexisNexis®
RISK SOLUTIONS
Balancing technology
and people

AML compliance spend is heavily skewed towards people rather than technology

People-related components (employment and training) dominate, accounting for almost 70 percent of AML compliance costs in the UK, compared to just under 25 percent relating to technology – see Fig 4. This is consistent with our Future of Financial Crime Research in 2020[7], which showed two thirds of AML compliance budgets were being spent on people-related costs, and only a third on technology.

On average firms reported having 38 full-time equivalents (FTEs) working on AML compliance in the UK, although for the bigger banks, this figure rose to over 100 FTEs.



Source: Oxford Economics

Fig. 4

An over-reliance on people renders firms vulnerable to challenges such as staff attrition and human error

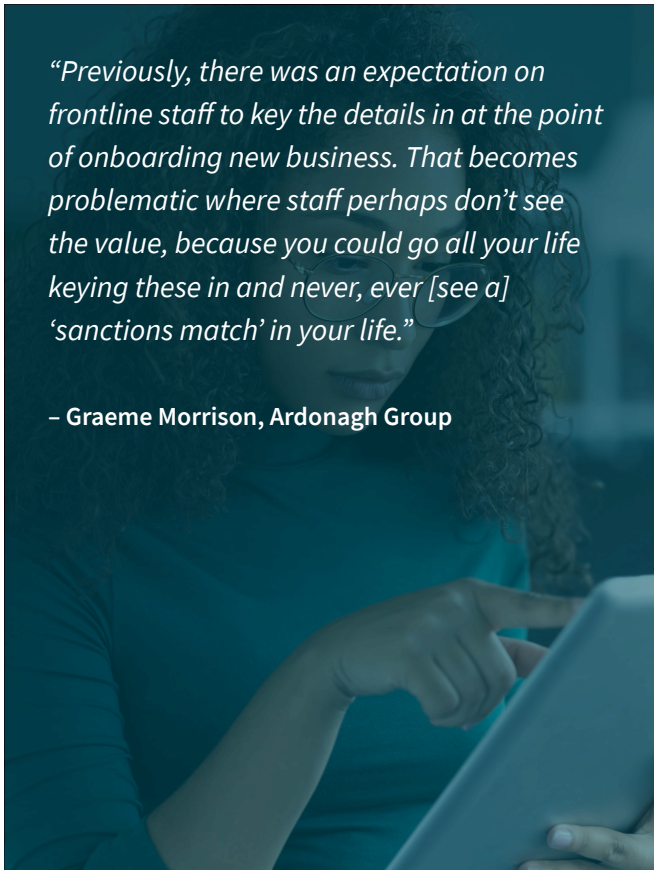
The biggest proportion of a firm's AML compliance costs relates to staff. Training staff and holding on to them can be difficult, especially given the high demand for financial crime compliance staff in the UK. If they are to be effective at spotting relevant activity and successfully preventing attacks, firms need to continuously ensure their compliance teams are fully briefed on all new and emerging criminal threats, yet, in practice, most AML related training is focussed on rules compliance and internal processes.

Keeping on top of fast-evolving criminal threats can be a real challenge, for example with the dramatic increase in malicious bot attacks and social engineering scams, or criminals infiltrating systems and client accounts, using different IP addresses and devices. It will come as no surprise therefore that almost 15 percent of total AML compliance budgets are being spent on staff training. Another issue relates to experience; ensuring frontline staff understand not only what they're being asked to do but also why, and what to look for.



"There is such big demand out there for compliance people, especially AML and KYC, you tend to find that people will jump ship quite often. This means that in many cases, compliance staff are not staying in roles long enough to achieve the necessary level of embedded learning into the commercial changes of financial crime trends that are occurring in that space."

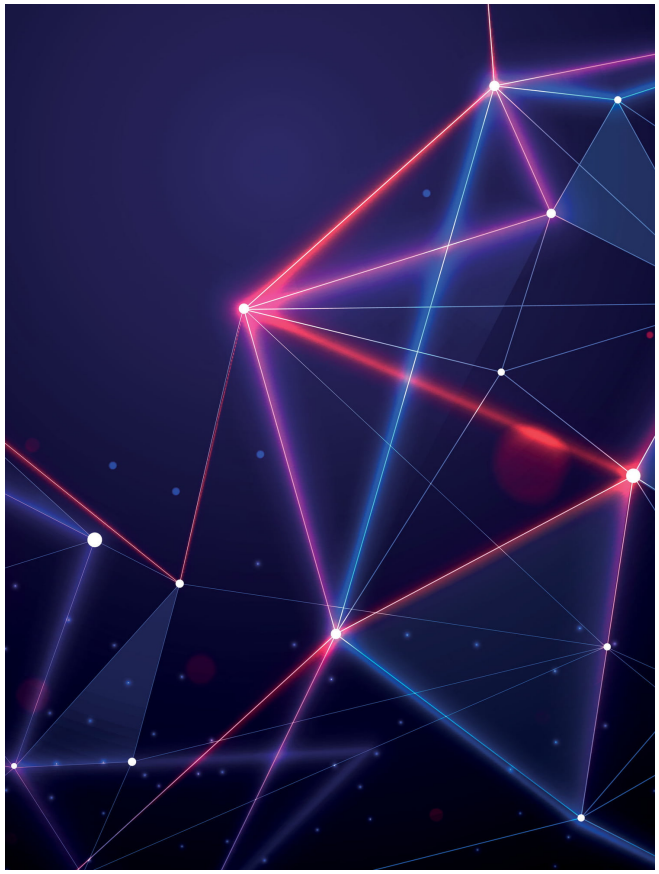
– Kam Biring, Currencies Direct



"Previously, there was an expectation on frontline staff to key the details in at the point of onboarding new business. That becomes problematic where staff perhaps don't see the value, because you could go all your life keying these in and never, ever [see a] 'sanctions match' in your life."

– Graeme Morrison, Ardonagh Group

Is it time to redress the balance and shift compliance spend towards technology rather than people?



Our respondents seem to think so...

Almost two in three firms experience problems with data quality; two in five experience issues with legacy systems; and a further two in five struggles with data silos. All of these issues contribute to unnecessary compliance activity and costs.

The reassuring news is, technology and data solutions are typically top of the priority list for firms aiming to improve AML compliance processes over the next three years, in particular, challenger banks and smaller financial institutions. Many large firms appear to be leading the charge in this regard, reporting strong performance in effective data management (91%), recent investment in technology (72%) and strong return on (technology) investment (81%).

In fact, according to our survey, there's a clear and strong direction of travel towards greater use of technology and data: Two in five (43%) firms are planning to launch data quality initiatives in the coming year, with a third (32%) planning to do so in the next two to three years.

Around the same number (39%) of firms will be implementing new compliance software this year, with a third (34%) looking to do so over the next three years.

41% of firms said they are looking to upskill their compliance staff with data science and technology capabilities over the coming year, with a further 31% of firms looking to recruit new staff with these skills within the same time period. The recruitment and upskilling of staff become even more of a priority for firms over subsequent years.

The pandemic has massively accelerated the shift to digitalisation. On average, respondents expect their technology costs to increase by 11.4% as a result of changing consumer habits and expectations.

Data and technology are already helping to reduce costs, but there’s much more scope



To understand the relationship between technology and future cost pressures, we modelled the relationship between the expected change in AML compliance cost and a firm’s current reliance on technology and data, as a share of costs.

Firms that report having more advanced technology and data systems also report lower compliance costs, all else being equal. These same firms expect compliance cost growth to be slower than for other firms, which suggests that data and technology is playing a crucial and effective role in helping firms to reduce the cost and burden of AML compliance, as well as mitigating future cost inflation.

Machines will never replace humans, but they can certainly support them

There's no substitute (yet) for applying good old-fashioned human instinct to properly risk-assess a case, as **Group Head of Financial Crime for a UK specialist lending bank**, explains. *"Systems are getting more capable of identifying some of the anomalies that you see; we're using systems to eradicate some of that increase in work, but it's difficult, especially with money laundering. You need that human interaction or intervention. You can put certain parameters in to help you identify what becomes a risk, but inevitably, there comes a final point where you need somebody to actually have a look at a case."* He adds, *"I think the idea of technology is to maintain the staffing levels rather than having to increase. It's not about reducing resource, it's just about managing your needs more sensibly."*



Technology and data can support process improvement



The majority of financial services organisations see scope for improvement in AML compliance process efficiency across the board, with around a fifth seeing an opportunity for significant improvements in relation to existing customer due diligence processes:

- Watchlist, sanctions screening and onboarding
- Identity authentication checks and risk assessment
- Ongoing monitoring of customers and payments
- Alert remediation and decisioning
- Investigation and reporting

Smaller organisations are more likely to see scope for improvement in each of the AML processes, with more than a quarter seeing large or very large scope for improvement in KYC identity authentication and watchlist and sanctions screening, as well as overarching activities.

Challenger banks in particular are aiming to improve data quality, with half launching data initiatives over the next three years and two in five (43%) updating compliance processes.

Intelligence-led, data-based analytics and AI are widely considered to be the future

The **Financial Action Task Force (FATF)** has indicated in its objectives for 2020-2022, that it will *"Prioritise work to tackle some of the great challenges facing societies around the world, including the opportunities that new technology offers to strengthen AML/CFT systems through digital transformation."* This includes a project aimed at helping the private sector make better use of artificial intelligence and big data analytics for AML/CFT.

So, what is stopping financial institutions in the UK from making better use of AI and advanced analytics?

- Legacy systems and infrastructure making it hard to take advantage of new technologies?
- A lack of understanding and knowledge of artificial intelligence, machine learning and natural language processing?
- Fear that the regulator will not fully endorse adoption of AI and analytics tools?
- Budgetary issues – the need to run legacy systems in parallel with new systems and techniques, and for smaller firms the initial cost of investment?
- Insufficient drivers for change – an embedded culture of rules-based compliance to satisfy the regulator rather than focusing on preventing dirty money entering the system?
- Lack of alignment within organisations between compliance and digital transformation strategies?
- Lack of vision as to the art of the possible – what can be achieved with big data and advanced analytics?

As the **MLRO of a leading UK bank** points out, one of the fundamental challenges is trying to move towards AI and analytics whilst simultaneously maintaining existing systems and controls. This inevitably causes the costs of financial crime compliance to increase considerably: *"You keep your old stuff running, and then you try to exploit new technology. That's quite a hard sell in terms of a board that's typically got a 12 to 24 month horizon."*



LexisNexis®
RISK SOLUTIONS

How can technology help?



How can technology and data support me in reducing the costs of AML compliance and improving the effectiveness of controls?

Assuming your organisation's approach to deployment is correct, new technology and better data management can help make AML screening more cost effective and, at the same time, reduce costs and manage financial crime risk more effectively. Such technologies constantly adapt to meet new AML regulatory requirements, allow for easy upscaling, and can help organisations to focus their people's skills more effectively, in doing the right things.

Unfortunately, in the pursuit of cost savings, organisations often take a sporadic and siloed approach to their KYC identity verification, AML screening technology and customer data management processes. This often leads to the mistaken conclusion that enriching risk data or using new technology, leads to an even greater workload in the form of dealing with higher volumes of alerts, remediating false positives, and unnecessary investigations.

However, the reality is that many firms are approaching this back-to-front. By addressing the accuracy and richness of your customer data across the organisation first, through effective Customer Data Management systems, firms will unlock significant downstream benefits and clear the way for powerful AI and risk screening technologies to create highly effective AML processes and help reduce the ever-spiralling costs of financial crime compliance.




LexisNexis®
RISK SOLUTIONS
Appendix

Appendix

[1] See next page for full Oxford Economics methodology

[2] https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file

[3] https://www.ukpublicspending.co.uk/uk_defence_spending_30.html

[4] For larger FIs with over £100bn AUM, the ratio of reported AML cost to AUM was 0.19, whereas for FIs with AUM from £500m to £1bn, this ratio shoots up to 1.58. For the smaller FIs (AUM less than £100m) the ratio is higher still, at 2.12.

[5] LexisNexis® Risk Solutions 5MLD research – average cost to implement 5MLD = £777k

[6] LexisNexis® Risk Solutions Sanctions and Alert Remediation report 2017

[7] LexisNexis® Risk Solutions Future Financial Crime Risks report



Survey methodology:

- Research carried out Oct Dec 2020, commissioned by LexisNexis Risk Solutions and executed by Oxford Economics.
- Telephone survey of 301 UK based financial services organisations (FSOs), including Retail banks, Challenger banks, Wholesale/Commercial banks, Investment banks/securities firms and money services businesses.
- Interviews with MLROs, or others with oversight of compliance activity across their UK operations.
- Objectives of the research:
  - Estimate the cost of AML compliance
  - Analyse the trends in costs, and potential factors influencing cost behaviour
  - Evaluate FSO's progress in implementing AML compliance best practices, and the impact of the pandemic on AML operations.
  - Identify potential actions, for FSOs themselves and regulators, to improve AML compliance efficiency and effectiveness

Methodology applied by Oxford Economics for estimating the total cost of AML compliance for UK Financial Services[1]

1. Surveyed 300 senior compliance officers across four key institution types to collect their estimates of the full cost of compliance, including people-related costs, technology and other administration costs, across their organisations (i.e. across all steps of the compliance processes from customer onboarding to exiting, in compliance functions and lines of business).

2. Calculated the median cost of compliance, to ensure our calculations were not distorted by outliers in the respondent sample. This results in a significantly lower, though more reliable estimate of the cost of compliance than using the mean.

3. Scaled the cost across the UK Financial Services sector using ONS statistics on the number of businesses in relevant sectors for different revenue bands. This arrives at an estimate of the total cost of compliance of £28.7 billion.

In some respects, this is a conservative estimate of the full costs of compliance of UK Financial Services, as some costs are not in scope of the calculation. For example we only scaled up for the institution types covered by the survey: retail banks, wholesale/commercial banks, Investment banks/securities firms and money services businesses, so are excluding other FS institutions that will have compliance costs, such as insurance companies and wealth managers. In addition, we excluded small institutions with annual revenues of less than £5 million. Although there are a large number of these small firms, they only represent 3% of industry costs.

LexisNexis®
RISK SOLUTIONS

How can we help?

Discover how our products and services could help you cut the cost of AML compliance

Learn More

Copyright © 2021 LexisNexis® Risk Solutions



POWERED BY Turtl