True Cost of Compliance 2023 | Report

Is the UK financial services sector doing enough of the right things to effectively fight financial crime?

LexisNexis®
RISK SOLUTIONS

Table of Contents

01

Is the UK effective in its efforts to detect, disrupt and deter financial crime?

Introduction

It has been four years since LexisNexis® Risk Solutions published a seminal report – *Money Laundering Exposed* – focusing on the damage wrought by money laundering on the UK economy and on the victims of the crimes that generate illicit gains. Much has happened since then: Covid-19, Brexit, and the war in Ukraine have exposed the UK to new mutations of economic crime (money laundering, fraud and corruption). In response, government, law enforcement and private sectors are combating the heightened threat with tougher legislation, increased resources and more public-private collaboration.

But the jury is still out on how effective these efforts have been in the fight against economic crime.

Figures suggest we're no more effective now than we've ever been, although there are no definitive measures. The National Crime Agency (NCA) estimates the cost of money laundering to the UK economy to be in the hundreds of billion pounds a year.[1]

According to the House of Lords: *"The UK is one of the most lucrative markets in the world for organised criminals. Billions are lost to fraud every year and an adult in England and Wales is more likely to become a victim of fraud than any other individual type of crime."*[2]

Regardless of the actual number, the belief of many is we're barely scratching the surface of financial crime in the UK, and perhaps only detecting as little as 1 per cent of the dirty money that passes through our national coffers.

[1] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance

[2] https://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/2022/november-2022/the-government-must-take-the-fight-to-the-fraudsters-by-slowing-down-faster-payments-and-prosecuting-corporates-for-failure-to-prevent-fraud/

Expert Perspectives

What is the current threat level to the UK economy and society as a whole from fraud and financial crime?
To find out, we asked three prominent figures* leading the UK's response to economic crime for their perspectives.

Nick Lewis, OBE

**MD Financial Crime Compliance,
Standard Chartered Bank**

Over the last three to five years, there's been a growing trend to include fraud in the definition of financial crime and that has changed the game completely.

We have much more of a partnership model than we've ever had and with the backing of the Economic Crime Plan, we've become global leaders, yet the vast majority of what we do is voluntary.

The big challenge of the day is, how do we dial down on the things that are less productive so that we can dial up on other things?

We've seen the evolution of some very good tools and technology, but the availability of the data unfortunately hasn't matched that pace. We need legislation that frees up the data so that these fantastic tools can really be let loose, both at home and across borders.

We need to think much more strategically about blocking channels, blocking financial flows and focusing on the enablers of money laundering. We need to understand what is it that attracts criminals to use a particular bank, product or services to move money.

The criminals will always be two or three steps ahead of us, and we're never going to be on a level playing field with them, but the last few years have shown us that even in times of real turmoil and trouble, we can keep public private partnership working, and that for me is our secret weapon.

Peter O'Doherty

**Assistant Commissioner – City of London Police,
and National Police Chiefs' Council Coordinator
for Cyber and Economic Crime.**

Until 2016, fraud wasn't even counted by the Crime Survey for England and Wales – now, it's the biggest individual crime in the UK!

Fraud and financial crime is among the most challenging to address from a law enforcement perspective. For one, the sheer volumes and the fact that over 70 per cent emanates fully or partially from overseas, meaning traditional law enforcement methods don't work against it.

Even understanding who owns the problem on a policing level has been challenging. Add to that the real danger of complacency, fueled by the misinformed rhetoric that financial crime is victimless and the lack of understanding of the impact, and you begin to appreciate the size of the challenge.

Much has been done in recent years to help define and understand impact, on a community, business and overall UK GDP level. But if the UK is to successfully reduce financial crimes, we need a proactive approach with common goals and priorities.

We can learn from and recreate successful information and intelligence sharing partnerships and build a cross-system people strategy to bring in the skills we need in the next 5 to 10 years, with a funding strategy to match.

We'll never prevent 100 per cent of financial crime, but we can definitely make a marked difference.

Nigel Kirby

Head of the Group Financial Intelligence Unit (GFIU) at Lloyds Banking Group and former Deputy Director for the Economic Crime Command in the National Crime Agency (NCA)

The past five years has seen a definite shift from economic crime compliance to economic crime prevention in the UK, with many regulated firms going well above and beyond with their voluntary, non-mandated prevention of economic crime activities, including those coordinated through the Joint Money Laundering Intelligence Taskforce (JMLIT). This indicates a clear change of perspective from doing what must be done to avoid fines and reputational damage, to doing what they believe is the right thing to do.

Real, targeted action against criminals can really make a difference. Working together as an industry in partnership with the National Economic Crime Centre and the Financial Crime Authority sharing data and knowledge will improve our joint understanding of organised crime threats. And we can then use that rich understanding to prioritise resources, improve preventative controls and increase the active disruption of criminals exploiting the UK's financial services.

Wider information sharing provides an equally rich opportunity. Advantage may be gained by supplementing law enforcement data with information held by telecoms companies, online retailers, or even internet providers. This whole system approach and sharing back intelligence with the financial services sector will assist us all to better protect our customers, our communities and the UK.

Above all, the economic crime ecosystem needs a collectively agreed, prioritised plan to tackle Economic Crime and then be bold and innovative in delivering it. We have data, we have skilled people – we now need real ambition and real system leadership.

*Nigel Kirby and Nick Lewis, OBE were also interviewed as part of the original 2018 Money Laundering Exposed Report

In summary

Those responsible for preventing and combating economic crime report that real progress has been made in the UK since 2018, but there's still a long way to go.

Much of the onus for detecting, disrupting and deterring economic crime sits squarely with industry; the financial services sector being at the heart of the ecosystem. So how are financial institutions responding to the challenge of preventing financial crime and, importantly, is it sufficient? Is it having the necessary impact? And what needs to happen in order for financial institutions to more effectively dial up on the activities and techniques that are having the biggest impact?

Research Methodology

We surveyed 300 individuals from different sizes and types of institutions across the financial services sector, probing for details of their compliance operations, including an estimate of the total annual cost of their financial crime compliance activities. We scaled up the average reported cost per firm to the total number of UK businesses (derived using business demography data from the ONS) to develop an estimate of the total cost of financial crime compliance across the UK financial services sector. The 2022 methodology has been updated to take into account differences between the AUM in the original 2020 sample. The median FCC cost per AUM is now calculated and applied to the median AUM size to calculate the median firm FCC cost. The study did not include smaller financial services firms with annual revenues of <£5m.

02

Is the UK financial services sector doing enough to fight financial crime?

Financial crime compliance spend for 2022 equivalent to three quarters of UK defence spend

Total financial crime compliance costs for UK financial services are estimated at £34.2 billion p.a., a significant increase of 19 per cent from the £28.7 billion reported almost two years earlier, and in line with the expectations of rising costs reported at the time, plus underlying cost pressures.

The total cost is equivalent to almost three quarters of the UK's defence budget for 2021/22 (£45.9 billion according to government statistics) – indicating that the sector is investing a huge amount of resource to meet the UK's financial crime compliance regulations.[3]

Our estimate of total costs is conservative and is based on the reported financial crime compliance spend of over 300 leading financial service organisations, which we then scaled up using ONS business demography data.* To reduce the influence of outlier responses we scaled up using the median reported cost.

*The figure does not include the costs of smaller UK financial services firms with revenues of <£5m

Compliance spend has risen since 2020, driven in part by rising volumes of activity

Even accounting for an 18.8 per cent growth in revenues across the financial services sector since 2020, financial crime compliance operational costs, as a proportion of revenue, have continued to rise over the period.

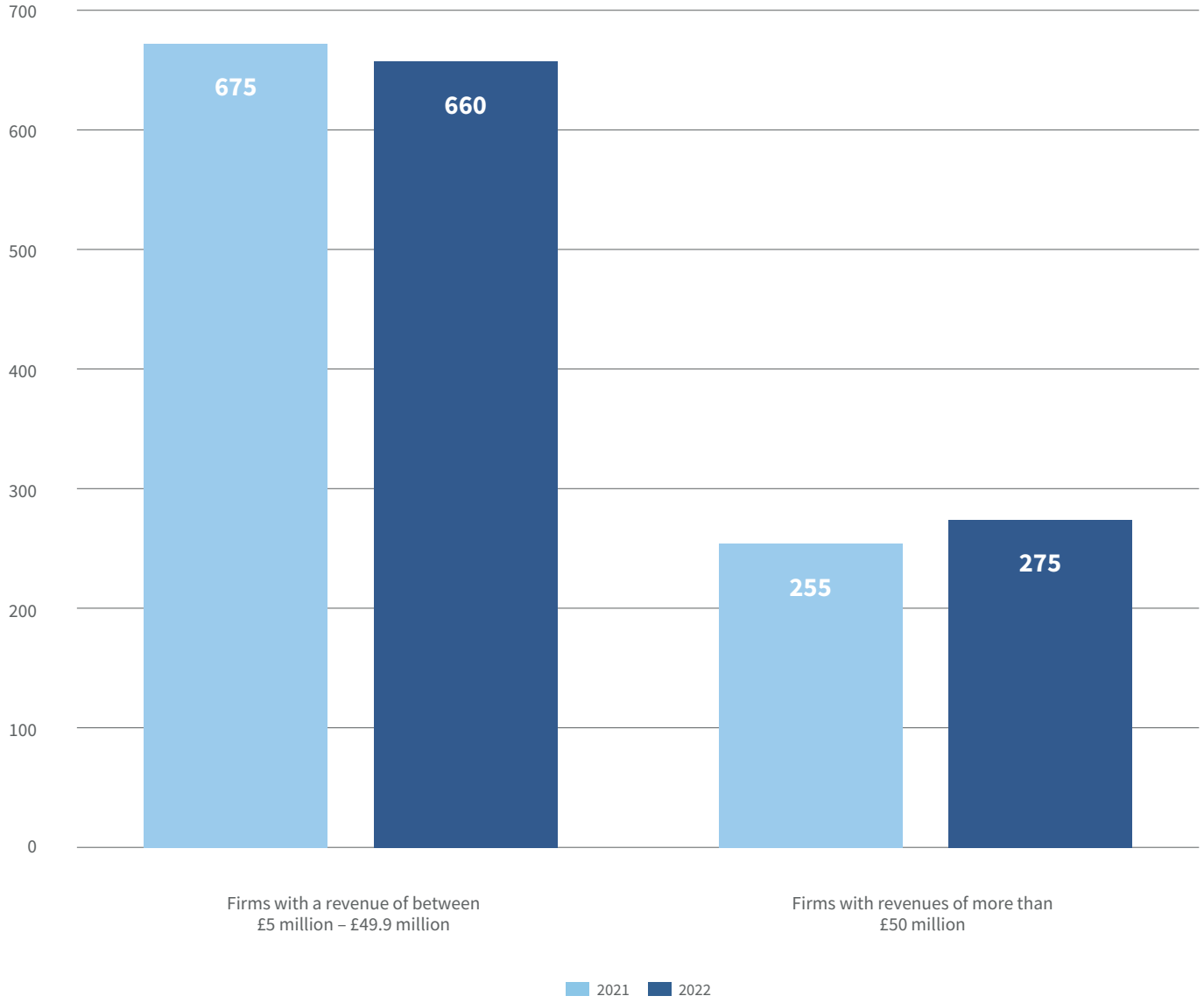
Adjusted for revenue growth, financial crime compliance costs are still 13 per cent higher than they were two years ago – above current inflation levels and in line with sector forecasts as revealed in our previous report.[4]

[3] MOD Departmental resources 2022: https://www.gov.uk/government/statistics/defence-departmental-resources-2022/mod-departmental-resources-2022

[4] The methodology has been updated to take into account differences between the AUM in the two research samples, for 2020 and 2022.

Fig. 1: Estimated total financial crime compliance cost

No. of firms

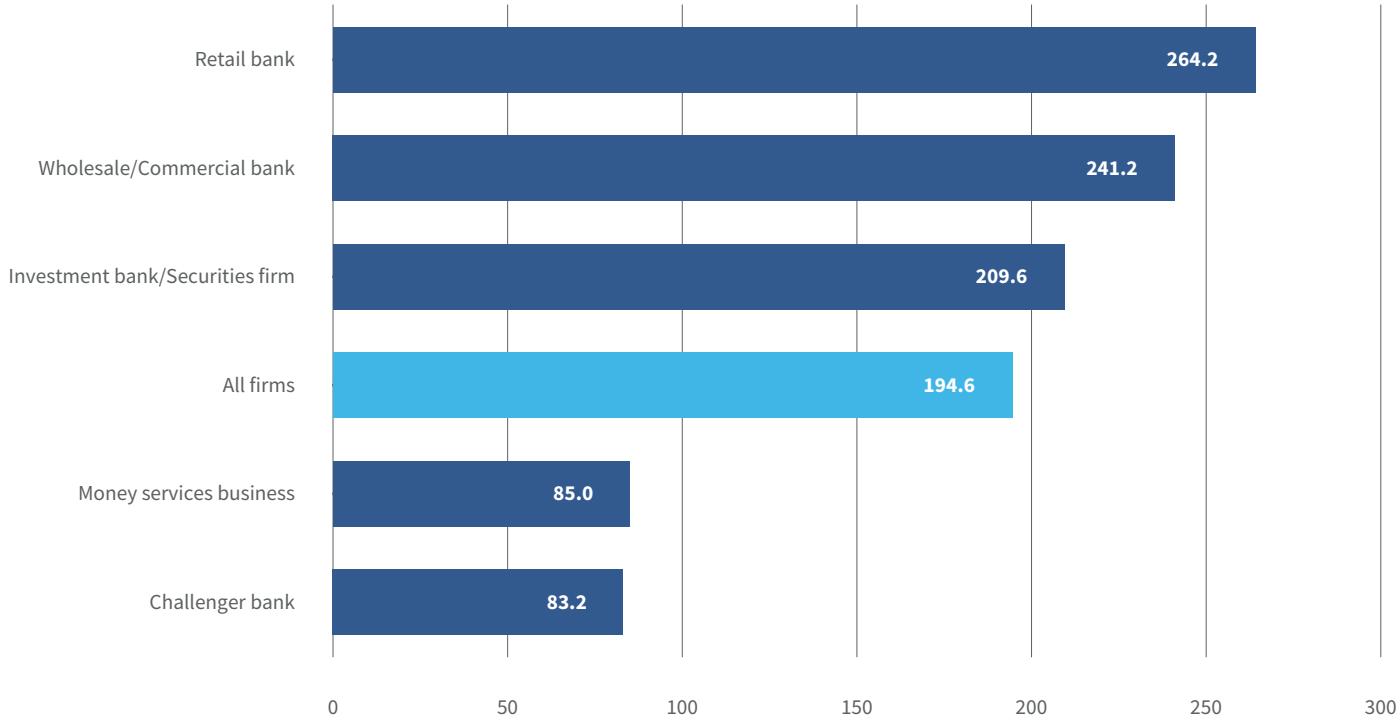


Compliance costs felt most acutely by smaller firms that lack economies of scale

The average cost of financial crime compliance, per firm, is £194.6m. However the impact of these costs is by no means felt evenly across all financial services segments – with smaller firms and certain other segments absorbing a higher impact on their margins. Financial crime costs for Retail, Commercial and Investment Banks track well above average, whilst costs for Challenger Banks fall well below the average.

The challenge of meeting regulatory and compliance requirements is revealed to be much tougher for smaller firms with revenues of less than £50m, which are seeing FCC costs equivalent to 2 per cent of their total revenue. For larger organisations the cost-to-revenue ratio is less than half a per cent (0.37 per cent).

Fig.2: Average reported cost of compliance by financial institution type*



n=300

Source: Oxford Economics

*Cost-weighted sample

Regulation remains the biggest perceived external compliance cost driver – more so than financial crime itself

As we found in our 2020 study, once again, increasing regulation and regulatory expectations are the greatest external drivers of cost, though other factors are also important.

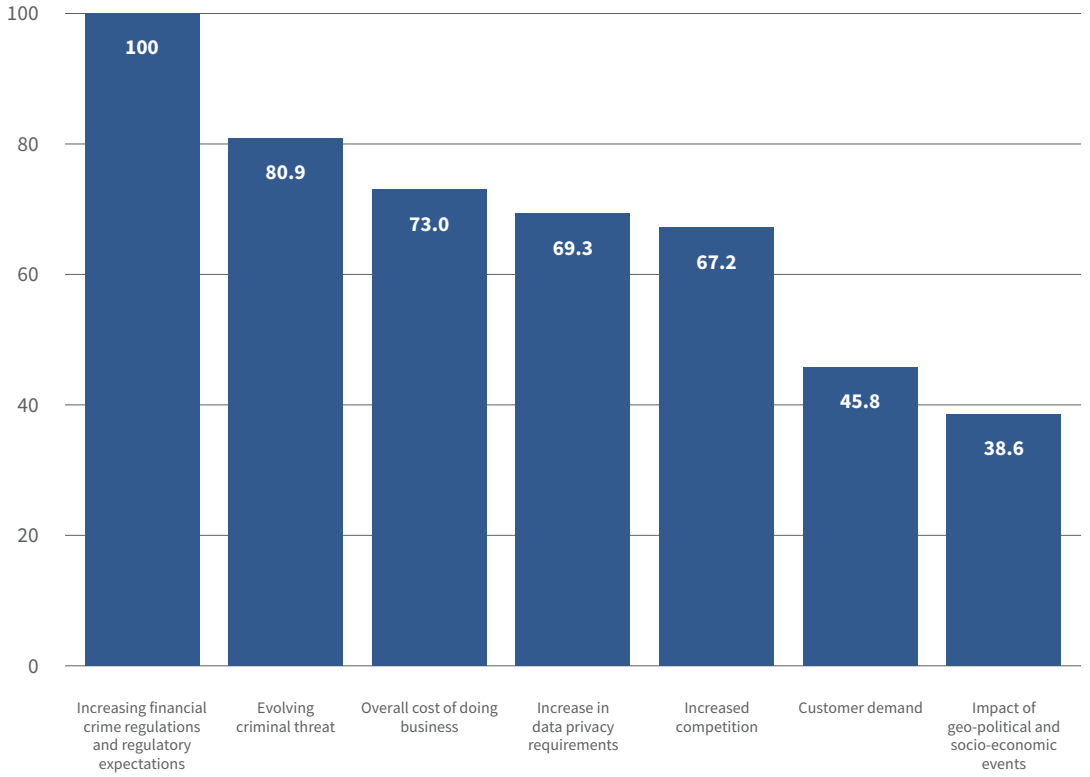
Whilst no new anti-money laundering (AML) regulation has come into effect since our last study in 2020, much has been updated including, introducing a travel rule for wire bank transfers involving crypto assets and changes in control of crypto asset firms, expanding the definition of trust or company service providers, clarifying the definition of art market participants and new powers – including information sharing powers – for AML supervisory authorities, such as the National Crime Agency. Further changes are anticipated in the coming months as the UK Government continues to beat its own path following Brexit.

Given that AML legislation hasn't changed substantially since our last analysis of compliance spend, it seems much of the regulatory pressure on costs is more about the fear of reprimand, rather than (or possibly as well as) the legal obligations themselves.

The regulators provide guidance for financial institutions to follow. Although it is merely 'guidance', nevertheless many firms are not prepared to take the risk of failing to follow it to the letter, leading to many firms going above and beyond what the legislation requires – known as gold plating.

Fig. 3: Perceived importance of external drivers of increased compliance costs*

Index value, highest perceived value = 100



n=273

Source: Oxford Economics

*Only firms which said their costs had increased vs three years ago: 273 firms out of 300.

Geo-political and economic factors are not significantly adding to compliance costs

Perhaps surprisingly, fewer than half (40 per cent) of respondents reported their financial crime screening costs have increased as a result of the Ukraine-Russia conflict, with those costs increasing by an average of 3.3 per cent.

Furthermore, geo-political and socio-economic events were cited as the least impactful external drivers of increased compliance costs, well below factors such as increasing regulation, evolving financial crime, the overall cost of doing business and increases in data privacy requirements.

Compliance costs are expected to continue rising by 2025

Aggregating responses and weighting by total cost, respondents expect overall financial crime compliance costs to increase by 8 per cent over the next three years.

Employee-related costs and investing in technology from external suppliers remain the largest two drivers of the forecasted increase in costs.

In summary

Financial institutions are spending heavily on financial crime compliance and this cost is expected to continue to increase.

Key questions to ask are whether this investment in compliance is leading to the desired outcomes in the fight against economic crime or whether some of this investment could be used more effectively to support other, more productive activities?

Another key question, given the slowdown in economic growth and with compliance costs expected to increase further, is whether this level of investment in financial crime compliance is sustainable?

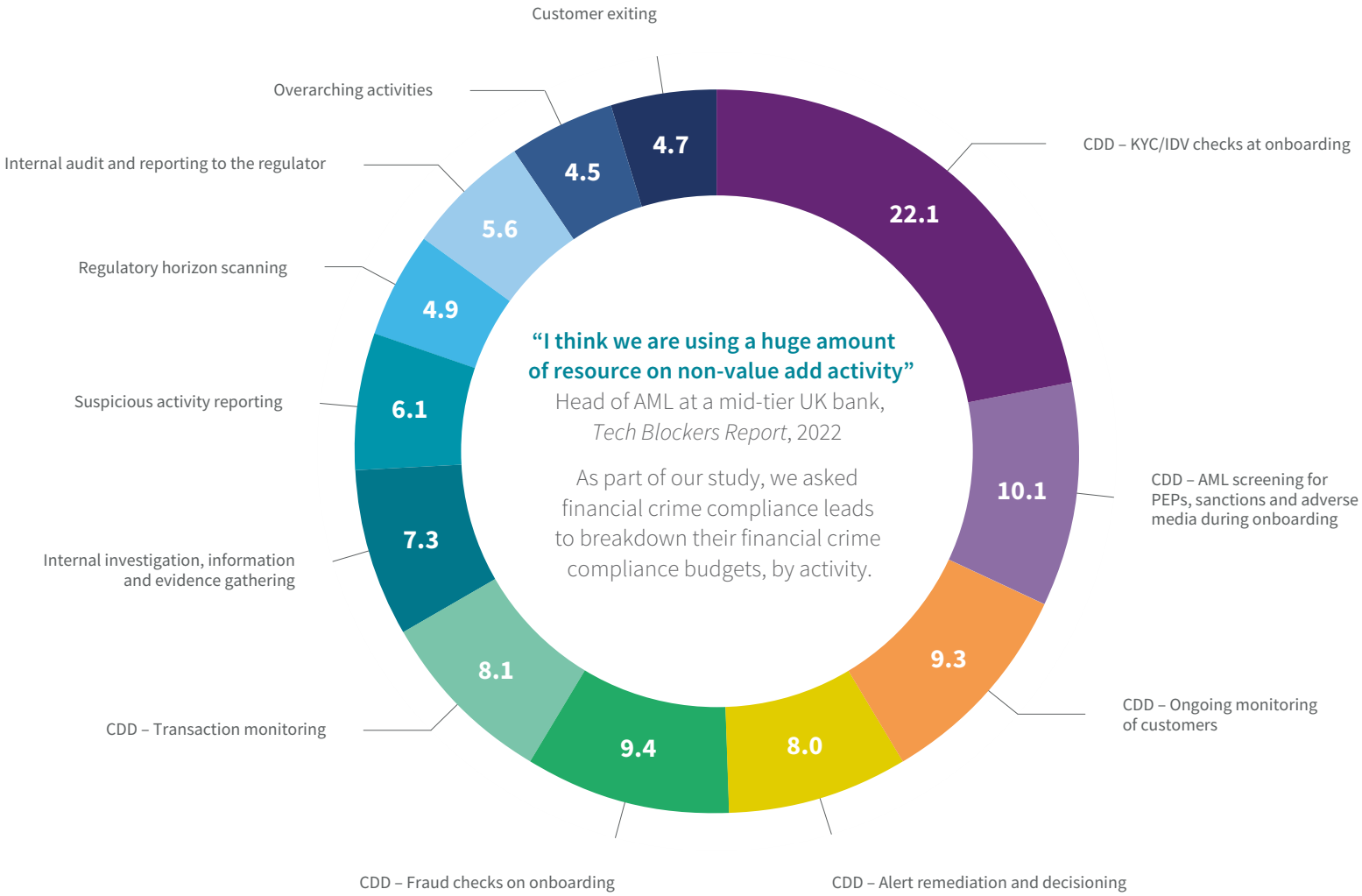
Is the industry reaching a tipping point?

03

Are UK financial institutions focusing on the right activities?

Fig. 4: Breakdown of financial crime compliance cost, per process*

Percentage share of costs



n=300

Source: Oxford Economics

*Cost-weighted sample

Customer due diligence activities are still consuming the majority of costs

Customer due diligence (CDD) processes remain by far the largest single operational cost, representing two-thirds (67 per cent) of total financial crime compliance costs in 2022, an increase from 53 per cent in 2020.*

The largest share of CDD spend is represented by Know Your Customer (KYC) onboarding checks, accounting for just a third of overall CDD costs. Anti-fraud checks at onboarding – necessary for the increased fraud risk posed by remote identity management and document verification – contributed to a further 9 per cent of CDD costs as firms move to strengthen their defences.

Beyond KYC, a further 10 per cent of compliance spend is consumed by AML screening, with another 8 per cent being spent on transaction screening and monitoring.

Firms also estimate that 8 per cent of costs are spent remediating alerts.

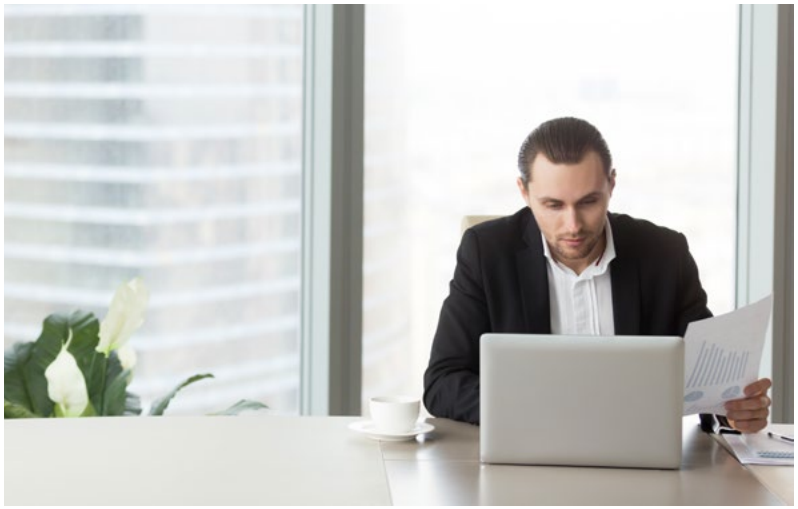
Normal deployment for onboarding, ongoing monitoring and transaction monitoring requires between six to eight separate systems for the average firm, potentially all with separate API callouts, requiring compliance teams to orchestrate within their own decision engine. The time and cost burden of brokering separate vendor agreements, the management of those vendor relationships and the maintenance of multiple systems, including API integration, and building and updating internal decisioning logic, is costly, especially when different systems don't talk to each other and where compliance teams are having to manually connect the dots to assess customer risk.

Expectations on firms to reflect improved financial crime detection in their KYC and AML processes has had a clear impact, with around a third of respondents reporting activity growth in internal investigations and another third in enhanced due diligence. This growth trend in investigations is even more pronounced in Challenger Banks and Money Services Businesses (MSBs).

Since 2020, regulators have been putting a much greater emphasis on the risk-based approach and the need for improved risk assessment processes with an appropriate level of due diligence. Many financial services organisations have either received a 'Dear CEO' letter from the Financial Conduct Authority (FCA) or else a reprimand from their particular supervisor, and fines continue to rise.

One well-known challenger bank we interviewed for our 2022 report, *Tech Blockers*, admitted the focus on faster onboarding and efficiency had led to them *"trying to rush through as many reviews as possible, which had a knock-on effect on the quality, and it is why we came under investigation."* This resulted in a backlog of investigations, which now need to be completed.

* The phrasing of the 2020 survey question was adjusted slightly for the 2022 survey to incorporate all financial crime screening as opposed to just AML screening activities, meaning the percentage increase will be skewed.



Biggest compliance volume increases seen in internal investigations and enhanced due diligence activities

Most respondents reported growth in volumes of internal investigations in 2022 (37 per cent), compared to enhanced due diligence checks (34 per cent) and DAML reports (31 per cent). Investigations overtook customer due diligence checks this year, which received the biggest volume increase score in the 2020 survey.

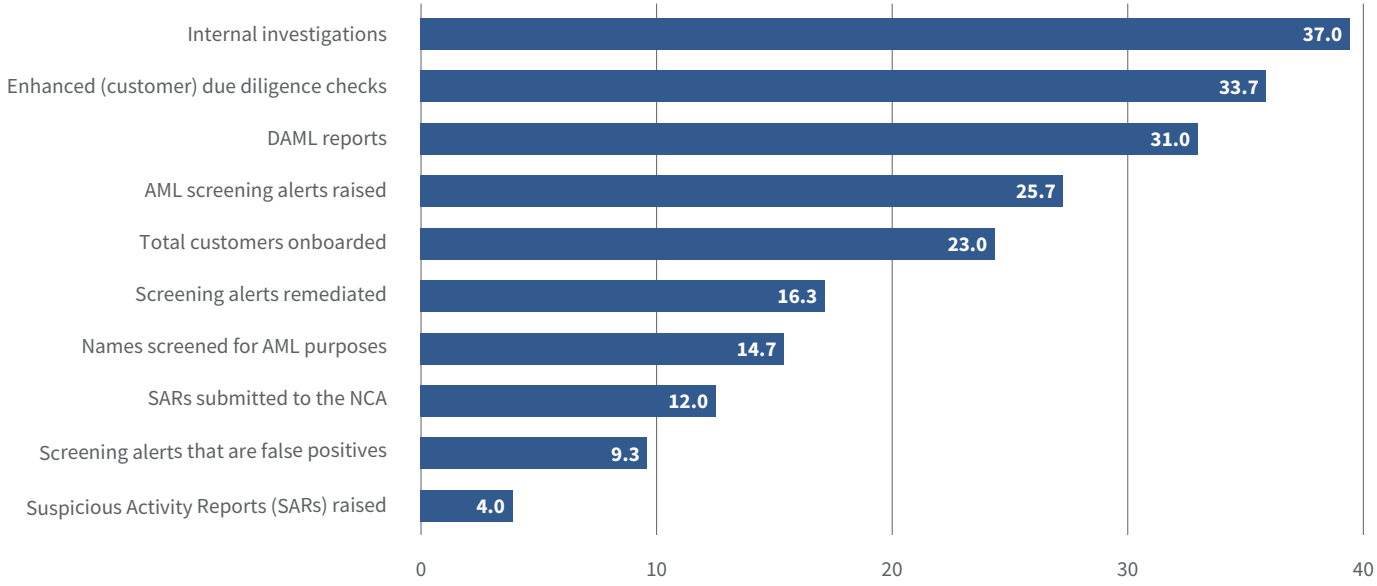
This trend is set to continue, with respondents expecting volumes of internal investigations to continue to grow more strongly than any other financial crime compliance activity over the next three years.

However, the effect of increasing internal investigations is not felt equally across all types of financial institution. Challenger banks and money service businesses were most affected, with investment banks, securities firms and retail banks seeing relatively smaller increases in the volume of internal investigations.

DAML reports now rank third, significantly higher than the 2020 survey where the net balance score was only 5 per cent.

Fig 5: Net balance of respondents reporting Financial Crime Compliance activity volume has increased

Share of respondents



n=300

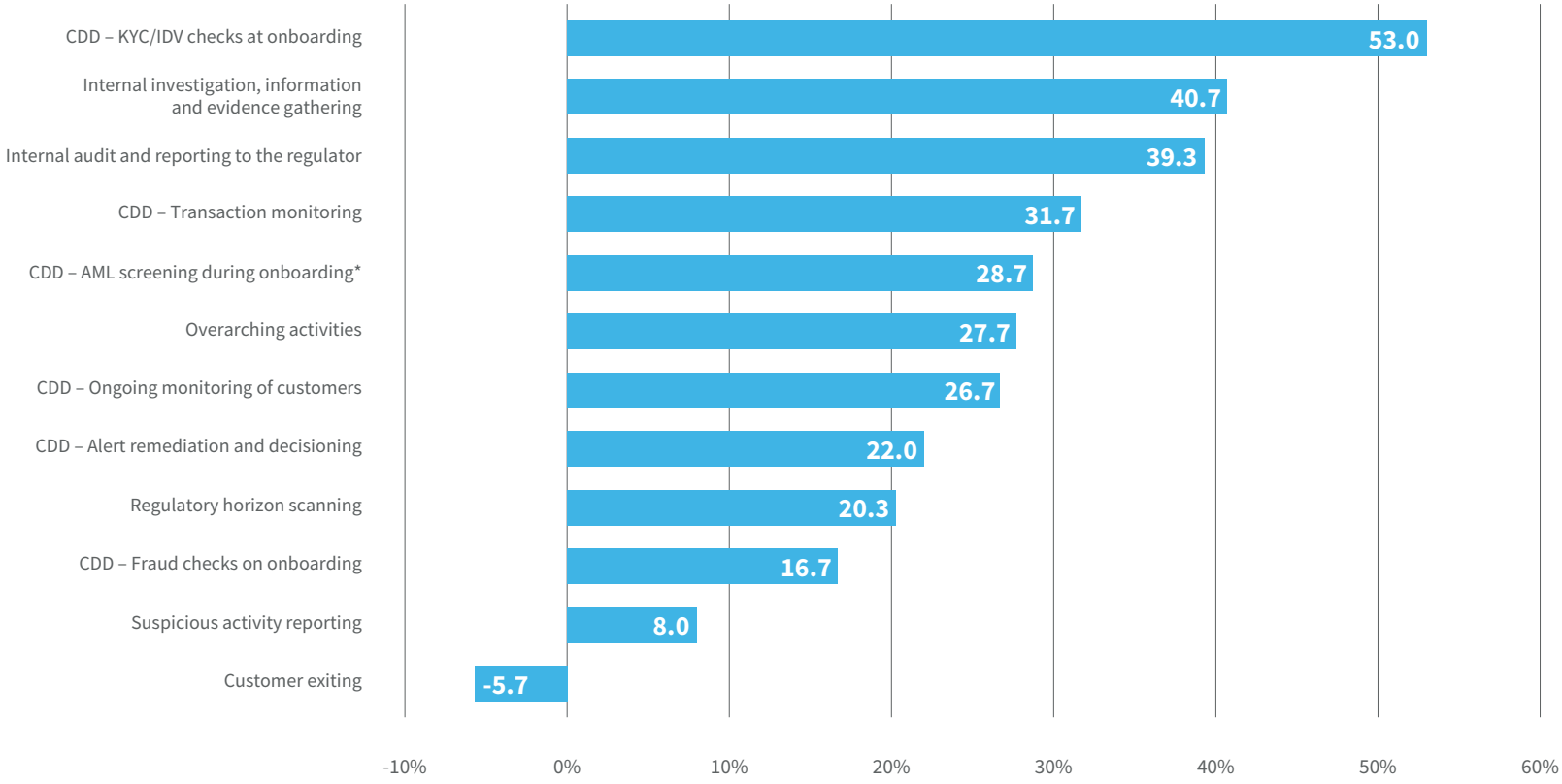
Source: Oxford Economics

Biggest compliance cost increases seen in KYC/IDV and internal investigations

Identity verification costs are also rising sharply, driven both by increasing customer volumes and by firms' efforts to improve their digital and remote onboarding solutions. More than half of respondents reported increased costs in this area, a trend driven initially by remote working, but more recently by competitive pressure, as more consumers demand a swift and seamless onboarding experience.

Fig 6: Net balance of respondents saying financial compliance costs are increasing

Net share of respondents



n=300

Source: Oxford Economics

*Screening for PEPs, sanctions and adverse media during onboarding

Main internal compliance cost drivers are increased automation, data, tools and new technologies, as well as growing financial crime compliance volumes

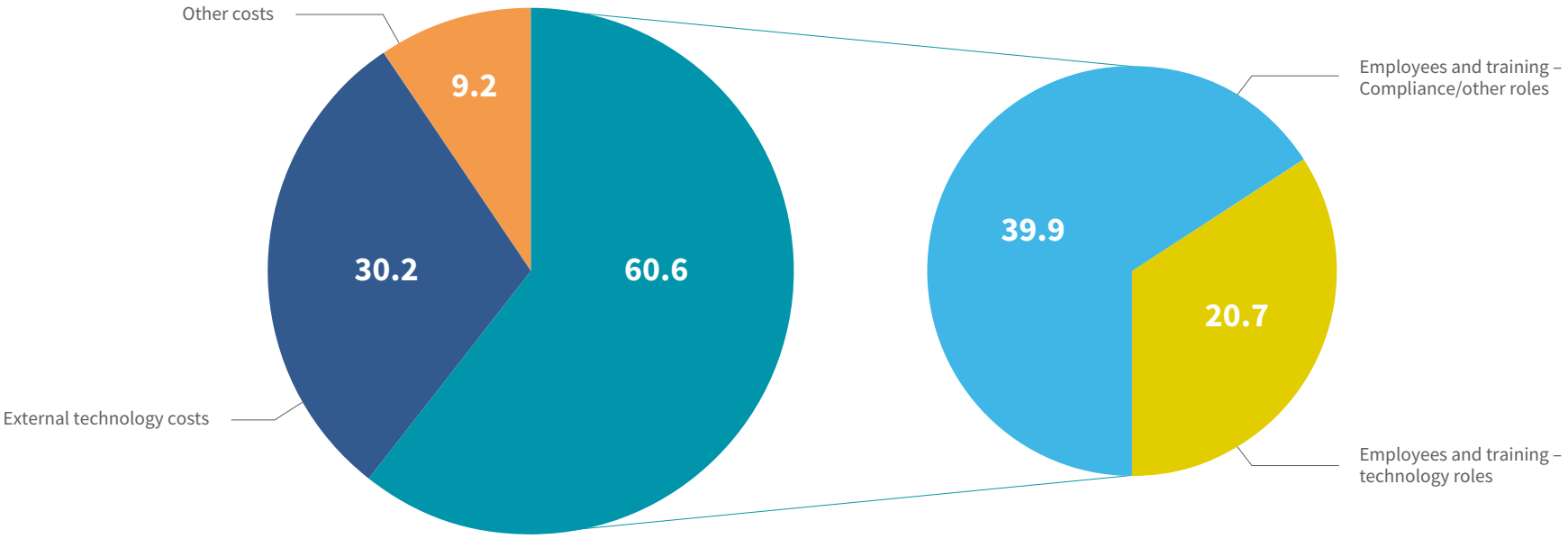
Respondents who experienced higher financial crime compliance costs over the past two to three years were asked about the internal drivers that contributed to this increase.

The main reason given was the increased requirement for automation and data to support compliance, just ahead of the growth in volumes of activity, which ranked top in 2020.

Investment in new technology and the costs of dedicated training for compliance staff were also cited as key internal drivers of increased costs.

Breakdown of FCC cost by Category*

Percentage share of costs



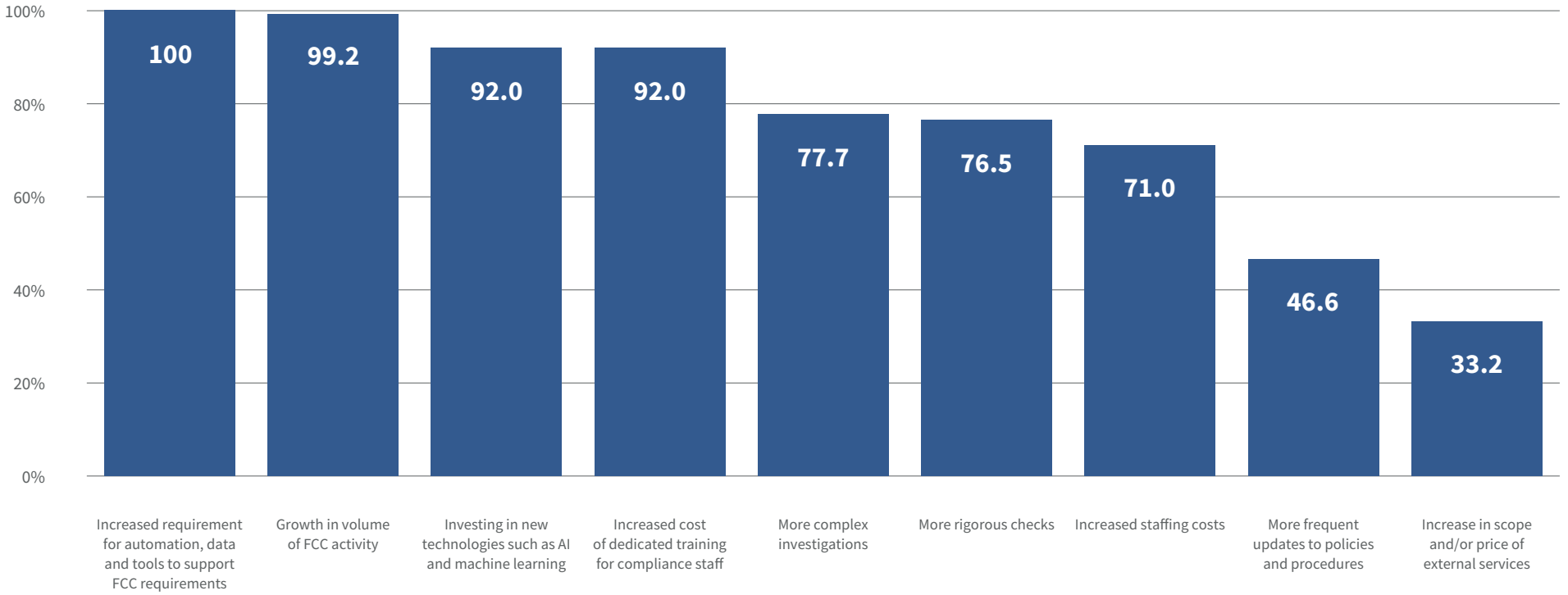
n=300

Source: Oxford Economics

*Cost-weighted sample

Fig 7: Perceived importance of internal drivers of increased compliance costs*

Index value, most significant factor = 100



n=273

Source: Oxford Economics

*Only firms which said their costs had increased vs three years ago: 273 firms out of 300.

Firms expect robust growth over next three years to drive more customers, more screening and more investigations

Figure 8 shows the net balance of respondents who reported that the volume of activity is expected to increase over the next three years, less those who reported a decrease.

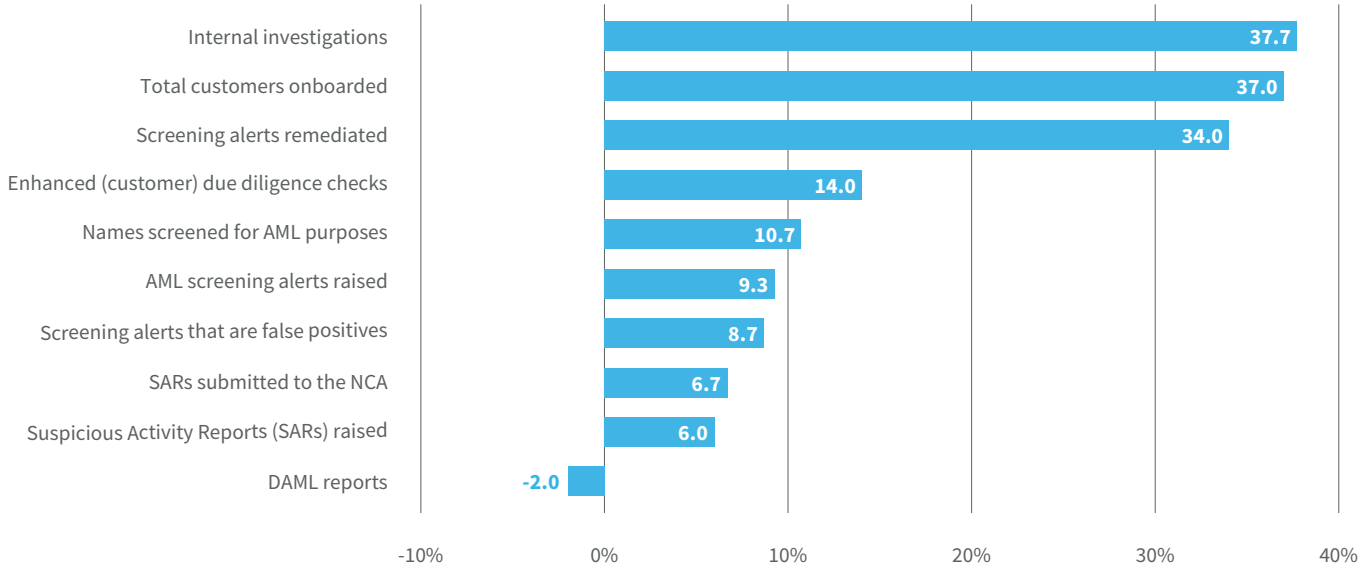
The data shows significantly higher expectations that investigations, onboarding and remediation activities will see the biggest increases in the next three years than for other related activities. Expectations for activity growth in internal investigations also received the highest net score for activity in 2019.

Businesses are expecting robust growth in the next three years, with total customers onboarded ranked second.

DAML reports are the only activity to see the net balance score turn negative when compared to 2019.

Fig 8: Net balance of respondents reporting that FCC activity levels are expected to increase over the next three years

Net share of respondents



n=300

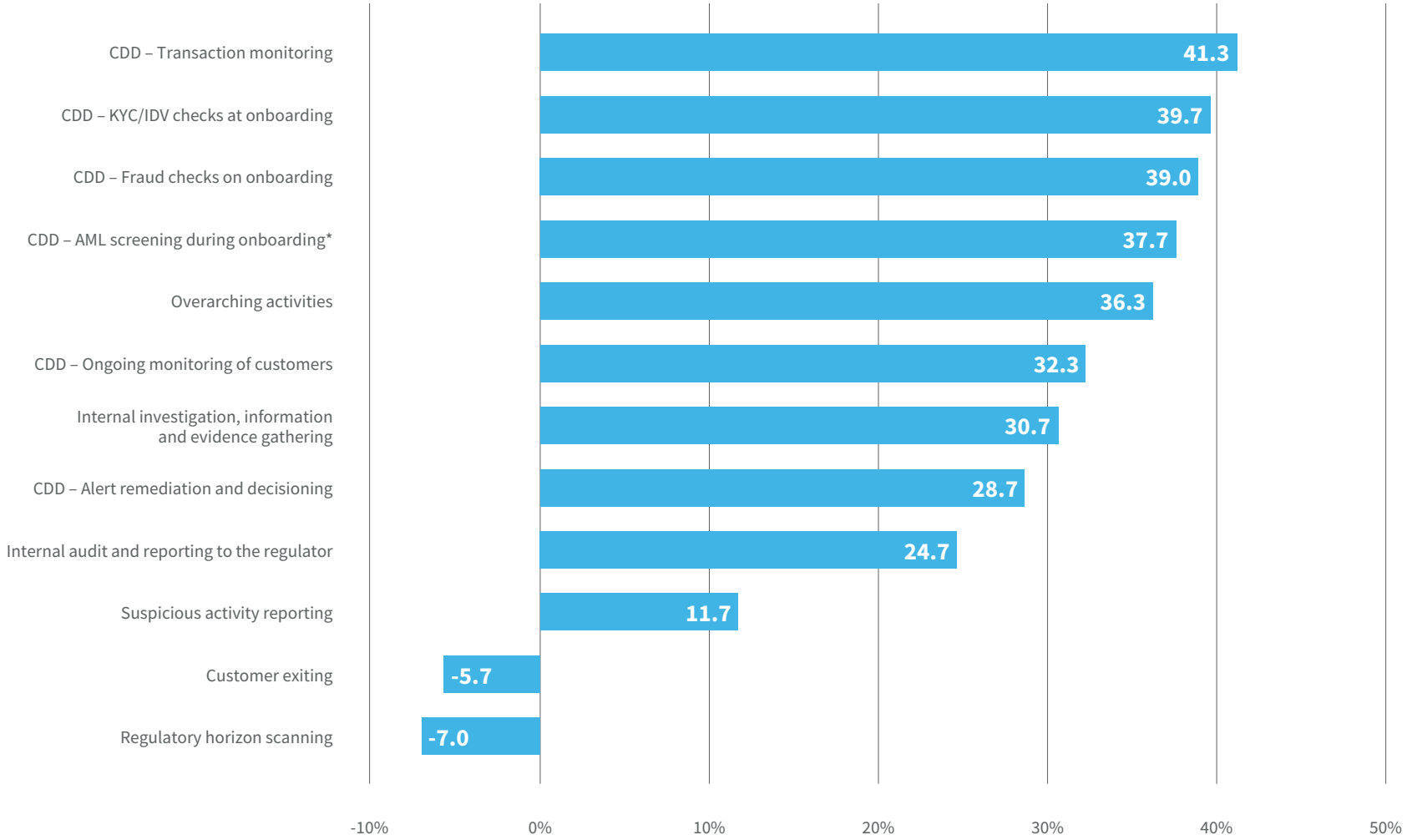
Source: Oxford Economics

Biggest cost commitments over next three years predicted to be transaction monitoring, KYC/IDV and fraud checks at onboarding

Looking forward to the next three years, respondents expect some of the biggest increases in financial crime compliance costs to come from transaction monitoring and fraud checks at onboarding, as well as KYC and IDV. In summary, the costs of customer due diligence checks have grown as a share of total financial crime compliance costs, now accounting for two thirds, despite more firms reporting increasing activity in internal investigations than compliance checks.

Fig 9: Net balance of respondents reporting that FCC activity costs are expected to increase in the next three years

Net share of respondents



n=300

Source: Oxford Economics

*Screening for PEPs, sanctions and adverse media during onboarding

In summary

The costs of customer due diligence (CDD) checks have grown as a share of total financial crime compliance costs, now accounting for two-thirds of spend, despite more firms reporting increasing activity in internal investigations than compliance checks.

Most firms expect financial crime compliance costs to continue to increase over the next three years, by an average of 8 per cent, with employee costs growing slightly faster than technology costs. This represents a slowdown from the higher growth reported since 2020.

Clearly more firms have begun their journey towards greater automation and digital transformation since we last surveyed them in 2020, however the increased spend on technology is evidently not yet translating into greater efficiency and cost savings. Firms will likely be anticipating a return on these investments in the coming years and should be reflected in future surveys.

Despite concerns around a slowing economy, nevertheless firms are anticipating robust growth, driving up volumes of customers for onboarding, screening alerts and internal investigations.

Costs are expected to increase the most around customer due diligence related activities; KYC/IDV and fraud checks at onboarding, and transaction monitoring.

04

Are the efforts of financial institutions having the necessary impact on financial crime?

Industry efforts felt to be somewhat effective, but with room for improvement

The view of most of the 300 heads of financial crime compliance we interviewed is that the industry response is making some positive difference, with two-thirds believing the UK financial sector is 'somewhat effective' and 28 per cent believing it is 'very effective' at detecting and preventing financial crime. Only around one in six respondents disagree, believing the UK financial sector's collective efforts to fight financial crime as 'ineffective'.

However, respondents were somewhat less convinced by their own organisation's response to financial crime, with just over half (57 per cent) describing it as 'effective'. A third of those surveyed rated the effectiveness of their organisation's response as 'average', while around one in seven went as far as rating it 'ineffective'.

Although over half of respondents overall said their own institution was at least somewhat effective, this was lower for challenger banks (50 per cent), possibly as a result of the recent FCA review, which may have led to a substantial overhaul of compliance processes.

The fact that the majority of firms think the industry is having a stronger impact on financial crime compliance than they are within their own organisation represents an interesting dissonance, suggesting compliance teams think their peers in other firms 'must be doing better' than they are.

On balance, many frontline experts believe their efforts to comply with anti-money laundering regulations is having some impact, but for most there is definitely room for improvement.

05

What improvements in financial crime processes have firms already implemented and what improvements do they expect to implement in the next three years?

Staff training and data improvement or augmentation

Financial institutions are making enhancements to their financial crime compliance processes and activities. Most recently, the principal focus for many firms has been on getting the right training in place for staff and investing in data improvement.

'Increasing the amount and quality of staff training' is the most commonly implemented improvement to date, with 45 per cent of firms having already implemented this.

Greater automation of CDD processes

Many firms are looking for greater automation of processes in order to cut costs, increase efficiency and free up time for their teams to focus on more value-adding activities.

Our research indicates that customer due diligence is already highly automated. Across our sample, firms had, on average, already automated over three quarters of the processes associated with customer due diligence. What's more, three in five respondents went on to say that they plan to further increase automation in customer due diligence, with KYC/IDV checks at onboarding and AML screening cited as the top two priorities.

By contrast, work associated with internal investigations, information and evidence gathering is significantly more manual. Certain sectors, such as retail banks have begun to meet this challenge, with 53 per cent indicating they have implemented partially or fully-automated investigations processes. Nevertheless, the very nature of this activity makes it harder to automate and therefore perhaps explains why investigations were cited as the lowest priority for automation in future.

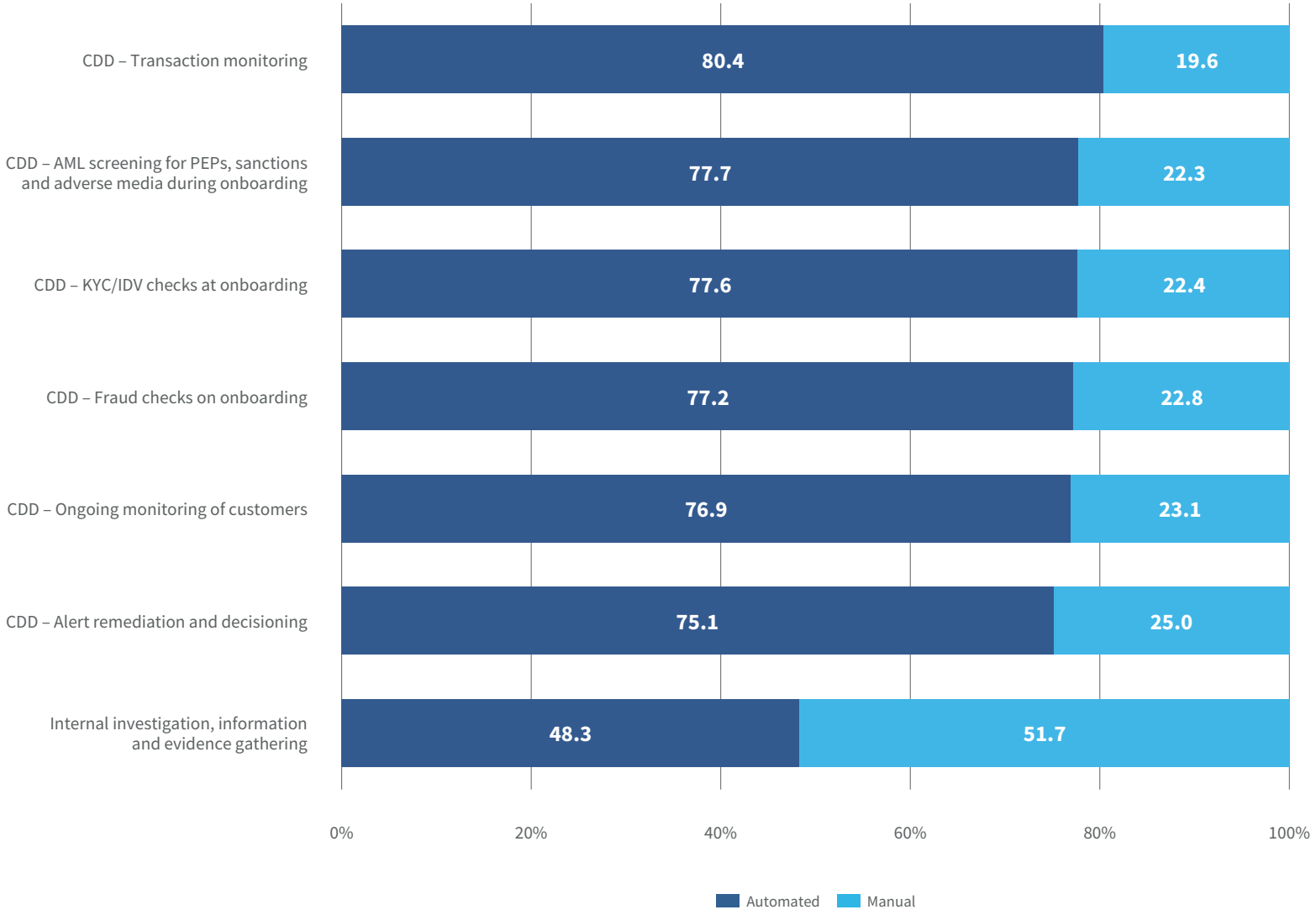
Increased integration of processes, activities and checks through FRAML and risk workflow orchestration

82 per cent of respondents expect to be converging fraud and financial crime compliance operations by the end of 2023. Merging fraud and AML functions promises to improve risk management as well as increasing operational efficiencies.

In support of this, there has also been a notable increase in the use of orchestration platforms to provide a full end-to-end solution for customer onboarding and ongoing monitoring, incorporating AML screening, transaction monitoring and case management within a single platform. Such solutions promise better customer experience through more dynamic risk ratings; lower costs and less time spent on the integration and day to day management of multiple data solutions across the risk workflow.

Fig 10: Average automation rate by process

Percentage automated vs manual



n=300

Source: Oxford Economics

Increased use of AI and advanced analytics

In 2020, the compliance industry response was largely 'people centred' with over 70 per cent of the outlay dedicated to employee and training costs. The big question now is whether the industry has learned to embrace technology solutions that can improve effectiveness as well as reduce overall costs.

The answer, it seems, is yes. Our latest research suggests encouraging trends towards significant investment in technology, with employee and training costs now accounting for around 60 per cent of spend and 30 per cent dedicated to the procurement of technology from external vendors. What is more, firms reported that on average, a fifth of their employment and training costs are spent on technology roles and training.

During 2023, the focus of many firms will be on increased adoption of new technologies such as Artificial Intelligence (AI), to be able to deal more effectively with larger volumes and to take advantage of sophisticated AI techniques such as machine learning, to help not only detect, but increasingly prevent financial crime.

As such, a key focus to date has been in building data science and information technology skills of financial crime compliance teams, either through training or recruitment. The success of AI relies on having the right skills in house to interpret the results, but it also relies on firms having sufficient and high-quality data. For some of the younger challenger banks and fintechs, this also requires a substantial investment in augmenting their data, so they have sufficient datapoints to be able to reap the full benefits of AI.

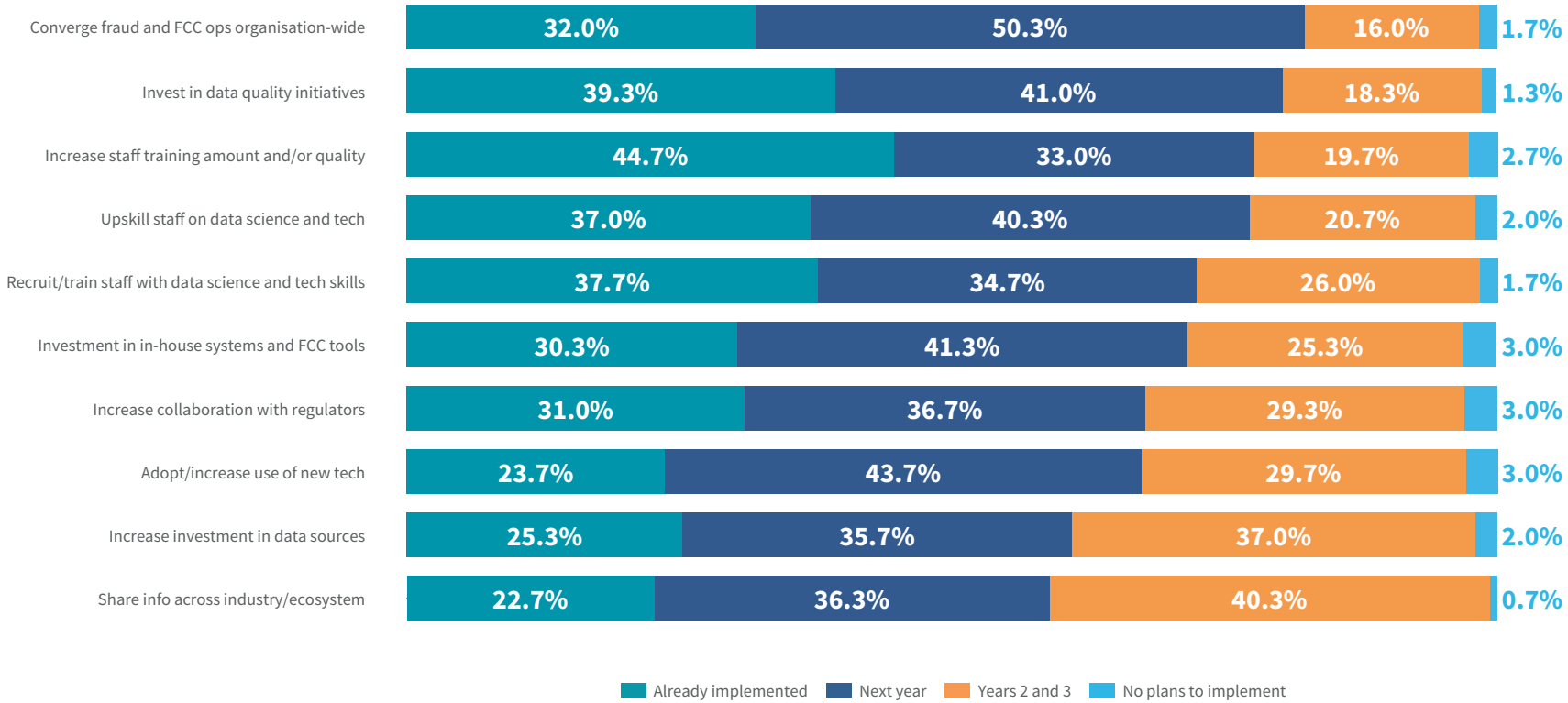
Broader sharing of fraud and financial intelligence

A slightly longer term, but nonetheless important enhancement planned by firms is to increase information sharing via consortia. By the end of 2025, almost all (99 per cent) firms expect to be actively sharing fraud and financial crime information in this way. It's almost universally accepted that greater information sharing powers and cooperation between public and private agencies would vastly improve the sector's ability to fight financial crime.

In summary

by 2025 firms expect to see tangible business benefits from their efforts, including improved data quality, increased volumes of high-risk customers detected, higher customer acquisition rates and better financial crime detection rates.

Fig. 11: FCC enhancements planned over the next three years



n=300

Source: Oxford Economics

06

Conclusion

Conclusion

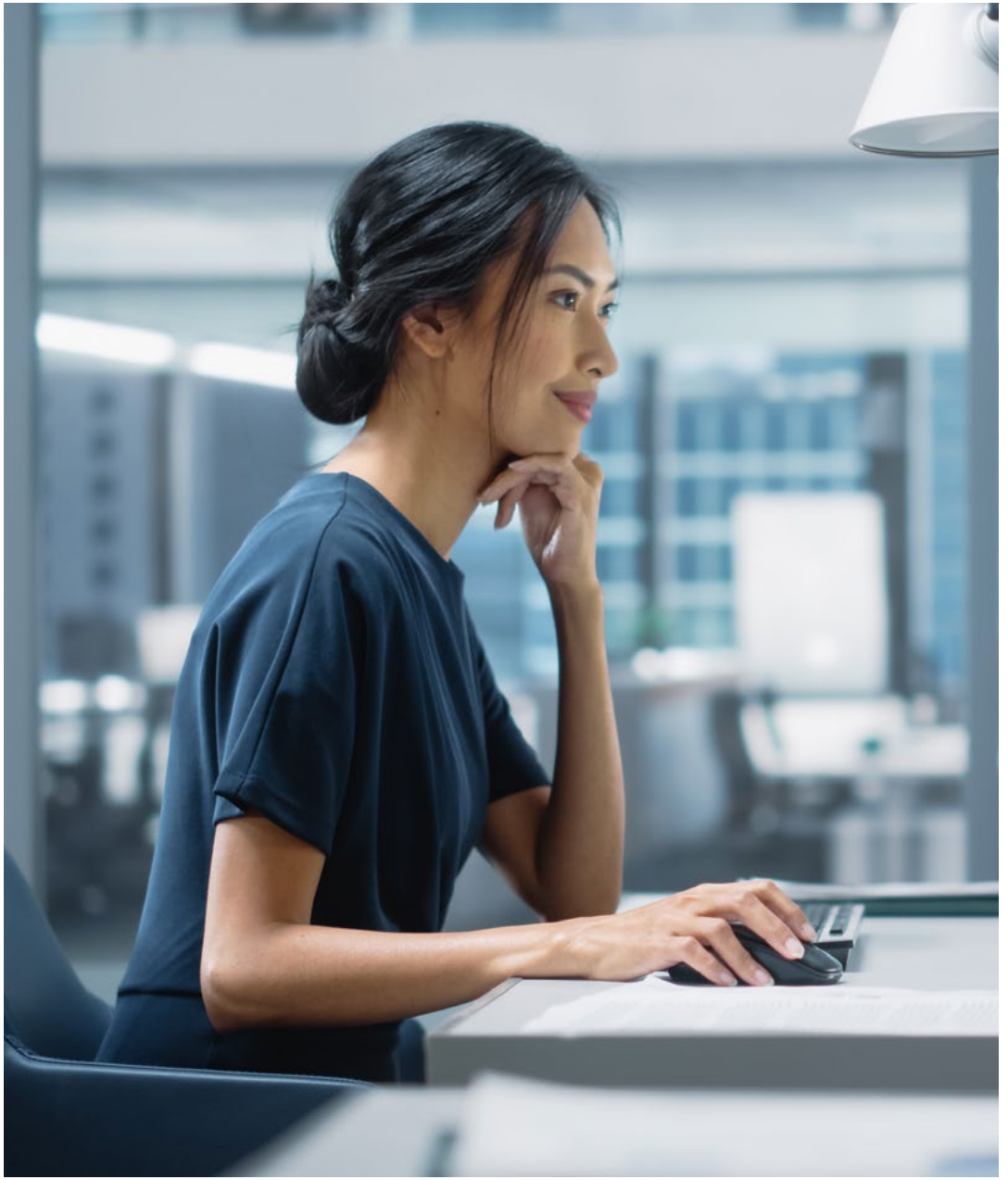
The cost of financial crime compliance – already a significant burden on the UK financial services sector – has grown further according to our latest study, by almost 20 per cent since 2020. The survey also indicates that firms expect these costs to continue to grow over the next three years.

Many of the drivers of this growing financial and operational burden are outside of firms' direct control; increasing regulation, an evolving criminal threat, and the increasing cost of doing business, among them. However, the survey points to many areas where management action can be taken to reduce costs and increase the effectiveness of UK firms' compliance activities.

Many firms have invested, or are planning to invest, in improvements to their financial crime compliance processes. Automation of customer due diligence processes is a key area, as is staff training. These enhancements are expected to deliver improved compliance, as well as other tangible business benefits, including better financial crime detection rates.

The survey indicates plenty of scope to improve financial crime compliance, both at an overarching and granular level. Given the huge costs being cited, even marginal efficiency improvements could amount to significant cost savings over time, with significant potential for improved competitive advantage and business performance.

The view that current legislation is failing to keep up with the rapid evolution of fraud and financial crime is a valid concern and many in the sector hope that regulators will soon consider a complete overhaul of financial crime policy, rather than continuing to tinker at the edges.



In the words of a respondent we interviewed for our *Tech blockers* report:

"I actually think we have too many bits of legislation and it's like putting another room on your house. But it gets to the stage where you need to knock down the house and start again."

The crux of the regulatory challenge lies in the ability to dial down on the activities that are less productive and value-adding, in order to dial up on those that are. Regulatory pressure and the need to 'keep the lights on' may be presenting a barrier to firms having the confidence to adopt a more common-sense approach and configure compliance activities in a way that they feel dials up on the most effective activities.

Responses to our study continue to underline the importance of a supportive, cooperative relationship with the regulator, one that encourages innovative thinking whilst providing reassurance against the threat of large fines if things go wrong.

Whilst there is still some way to go before the financial services sector can proclaim to be truly effective at detecting and preventing financial crime, evidence from this study suggests that the next few years will be seminal in that journey. Greater automation, adoption of advanced analytics and AI, collaboration and information sharing and a stronger relationship with supervisory bodies all promise to help transform and shape a new way of tackling financial crime. Increasingly, the limitations of a siloed approach are being realised. Unless this changes, and we push for wholesale transformation in the way financial crime is tackled, the figures presented in this report suggest that a tipping point will soon be reached by the industry, whereby every extra Pound spent on compliance will have no additional impact on effectiveness. No one – not industry, not government, not society, can afford for that to become a reality.

To find out how LexisNexis® Risk Solutions can help,
contact our team on 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions is a leader in providing essential information that helps customers across all industries and government assess, predict, and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information and analytics for professional and business customers across industries.