



ON THE FRONTLINE

THE UK'S FIGHT AGAINST
MONEY LAUNDERING

MONEY LAUNDERING
EXPOSED

Written by

**The
Economist**

**INTELLIGENCE
UNIT**

FOREWORD

Behind every money laundering scheme there are victims entangled in drug trafficking, modern slavery, gang crime, violence and cybercrime.


The perpetrators of these offences are criminals, but they are also smart, technologically advanced, and hiding in plain sight. They operate outside of the law and are not held back by regulation, jurisdiction or policy. Meanwhile, those battling against financial crime are constrained by limited resources, regulated intelligence and restricted cross sector collaboration.

This report focuses on business and the AML professionals in regulated sectors—our frontline in the UK’s fight against money laundering—in order to gauge their views on the issues and concerns, to assess their appetite to make a difference and to determine whether they feel they have the right tools and support to do the job.

Our sincere thanks go to the Economist Intelligence Unit*, who produced this paper on our behalf, and to the interviewees and survey respondents who gave up their time to provide us with insights from the front.

With such wide-ranging impacts, money laundering should no longer be considered a white-collar crime. It affects lives. In some cases, it kills. This paper aims to drive not only conversation, but action.

* Please note this report alone was written by the EIU. The EIU is not responsible for other content in the ‘Money Laundering Exposed’ initiative.



THE BANKING INDUSTRY ALONE
SPENDS BILLIONS PER YEAR²
ON PEOPLE AND SYSTEMS TO
PREVENT, TRACK AND REPORT
ILLICIT MONEY FLOWS, YET
ONLY A VERY SMALL FRACTION
OF LAUNDERED MONEY IS
EVER STOPPED OR RECOVERED.

INTRODUCTION

With potentially more than £100bn¹ in illicit funds impacting its economy each year, the UK lies at the heart of the fight against financial crime. Despite significant investment, anti-money laundering (AML) enforcement successes are limited. The banking industry alone spends some £5bn per year² on people and systems to prevent, track and report illicit money flows, yet only a very small fraction of laundered money is ever stopped or recovered.

This report investigates how well frontline, regulated firms feel the UK's AML regime works. It also gauges the level of commitment to stamping out money laundering, from the C-suite to branch office.

The survey, conducted by The Economist Intelligence Unit on behalf of LexisNexis® Risk Solutions, details where the risks lie and how government policy, regulation, internal procedures and technology can best be deployed to ensure the private sector and enforcement agencies can counter flows of dirty money in, around and out of the UK.

The Economist Intelligence Unit is grateful to the following senior AML executives from across the banking and financial technology sectors for their thoughts and insights.

- Brian Dilley, group director of fraud and financial crime prevention, Lloyds Banking Group
- Paul Kilbride, chief compliance officer and money laundering reporting officer, Secure Trust Bank
- Erik Morgan, managing director, global due diligence, governance and regulatory solutions, RBC Investor & Treasury Services
- Ben Steyn, head of compliance, Transferwise
- Natasha Vernier, head of financial crime, Monzo Bank

1. National Strategic Assessment of Serious Organised Crime, National Crime Agency, 14 May, 2019, https://issuu.com/nca_uk/docs/official_nsa_-_final_for_web_8d54fba93a80de?e=38089831/69834688

2. BBA response to Cutting Red Tape Review – Effectiveness of the UK's AML Regime, British Bankers' Association, 6 November 2015, <https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime/>

**MONEY LAUNDERING IS
CLEVER, TECHNOLOGICALLY
ADEPT AND CHANGING FAST
IN THE DIGITAL WORLD.**

EXECUTIVE SUMMARY

THE GROWING THREAT OF MONEY LAUNDERING

Evolving criminal methodologies are the single biggest risk in the UK's fight against money laundering according to 24% of respondents. Money laundering is clever, technologically adept and changing fast in the digital world. Although the UK's AML regime is responding to these threats, it is still unable to completely stamp out financial crime.

THE APPETITE FOR BATTLE

Inconsistent AML controls across industries (cited by 42%) and a confusion of regulators (24%) often leave companies feeling they work in silos (46%). Regulated businesses are uncertain about where to direct their concerns and whether the information provided by their Suspicious Activity Reports (SARs) is used. The return on investment from their AML compliance, with costs rising, is hard to evaluate. Even so, banks, financial technology, (fintech) firms, lawyers, estate agents, accountants and the gambling operators want to improve the efficiency of their AML efforts, but feel they lack the appropriate guidance to do so.

PREPARING FOR COMBAT

Respondents want clearer (36%) and more frequent (30%) communications between regulators and regulated business. Regulated firms need to adopt a zero-tolerance approach, through training and a company-wide focus on detecting and reporting suspected financial crimes. Government and enforcement agencies, notably the National Crime Agency (NCA), need to help frontline firms and staff, particularly as laundering methodologies change rapidly in the digital world.

CLEARING THE OBSTACLES

Nearly a third of respondents believe better monitoring and reporting of enforcement outcomes would be the most efficient way to boost AML. Hundreds of thousands of SARs are submitted, at substantial cost to regulated firms, but their quality is questionable, while crime agency units are too overstretched and under-resourced to efficiently make use of the information. Other conflicting rules and legislation, on data, confidentiality and collaboration, could be reworked.

COMMUNICATE, CO-OPERATE

According to respondents, increasing information sharing between company departments (42%) and between regulated businesses (37%) is the key to better AML. Money laundering teams should be able to share their concerns earlier with their peers and across sectors, if they are to successfully eradicate criminal activities. Legislators and regulators should be more transparent and realistic in their guidance on best practice and in the use of technologies designed to track transactions, individuals and unusual behaviour.

AN INDIVIDUAL COUNTY LINES GANG, KNOWN TO TRAFFIC AND EXPLOIT VULNERABLE CHILDREN, CAN MAKE PROFITS IN EXCESS OF £800,000 PER YEAR FROM DRUG DEALING.³

• IN THE UK, MORE THAN £190,000 IS LOST EACH DAY BY THE VICTIMS OF CYBERCRIME.⁴

THE NATIONAL CRIME AGENCY (NCA) STATES THERE IS A REALISTIC POSSIBILITY THAT THE SCALE OF MONEY LAUNDERING IMPACTING THE UK IS £100BN+.¹

• IN 2018, THERE WERE 83,864 VICTIMS OF AUTHORISED PUSH PAYMENT SCAMS REPORTED BY UK FINANCE MEMBERS.⁵

• 6,993 POTENTIAL VICTIMS (INCLUDING 3,137 MINORS) OF MODERN SLAVERY/HUMAN TRAFFICKING WERE FLAGGED IN THE THE UK IN 2018.⁶

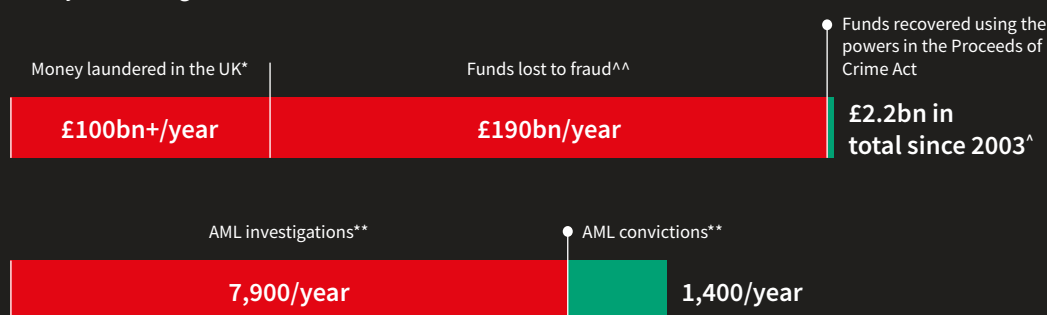
CHAPTER 1: THE GROWING THREAT OF MONEY LAUNDERING

Nobody really knows how large a problem money laundering is in the UK.

The National Crime Agency (NCA) states there is a realistic possibility that the scale of money laundering impacting the UK is £100bn+.¹ There is also a reported £190bn lost to fraud,⁷ the most common crime suffered by British citizens—the proceeds of which need laundering too.

The UK also remains an attractive destination for politically exposed persons (PEPs); these are people who may be susceptible to bribery and corruption. Often, PEPs buy high-end assets through complex transactions involving shell companies and nominee ownership. This can allow them to bypass the requirement to register People with Significant Control (someone holding more than 25% of shares or voting rights in a company, or having the right to appoint or remove the majority of the board of directors), which has been on the books since 2016.⁸

Figure 1
Money laundering in numbers



Source:

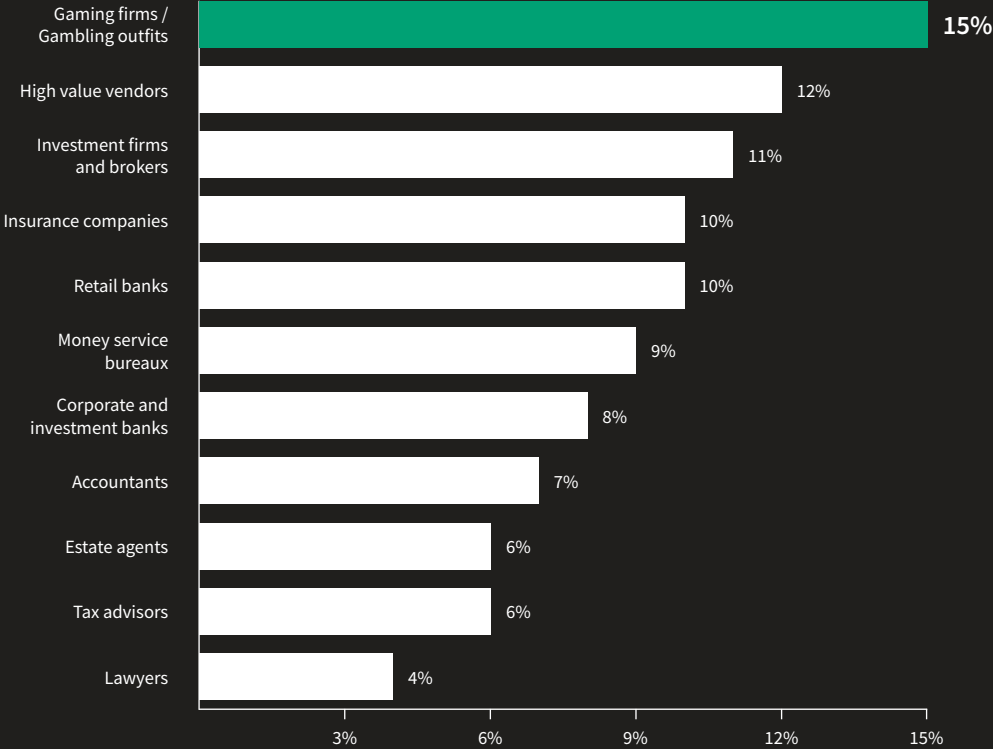
- * National Strategic Assessment of Serious and Organised Crime 2018, National Crime Agency
- ** Anti-money laundering and counter-terrorist financing measures-United Kingdom-Mutual Evaluation Report, Financial Action Task Force, December 2018
- ^ Economic Crime Factsheet 2017, Home Office
- ^^ Annual Fraud Indicator, 2017, University of Portsmouth Centre for Counter Fraud Studies/Crowe UK/Experian

SECTORS AT RISK

Although banks and building societies represent the bulk of flagged suspicious transactions, the regulated industries' perception is that criminals are most likely to target the gambling sector (cited by 15% of respondents) and high-value vendors who accept large cash payments (12%).

3. NCA County Lines Drug Supply, Vulnerability and Harm 2018, <https://nationalcrimeagency.gov.uk/who-we-are/publications/257-county-lines-drug-supply-vulnerability-and-harm-2018/file>
4. BBC News Report 'UK cyber-crime victims lose £190,000 a day', <https://www.bbc.co.uk/news/uk-47016671>
5. UK Finance, Fraud the Facts 2019, <https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019>
6. National Referral Mechanism statistics – End of Year Summary 2018, <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/282-national-referral-mechanism-statistics-end-of-year-summary-2018/file>
7. Annual Fraud Indicator, 2017, Experian/University of Portsmouth Centre for Counter Fraud Studies/Crowe UK, <https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Annual-Fraud-Indicator-report-2017>
8. 'People with Significant Control' Companies House register goes live, <https://www.gov.uk/government/news/people-with-significant-control-companies-house-register-goes-live>

Figure 2
 Sectors most at risk of money laundering? (n=204)



Brian Dilley, group director of fraud and financial crime prevention at Lloyds Banking Group, agrees that high-end vendors need to be alert, but thinks expensive London townhouses are likely to be the prominent end-story of laundered money. “Art and property are bought by the ultra-wealthy organised crime groups with the concentration of money they have got from smaller operations,” he says.

Perhaps surprisingly then, only 6% of respondents view estate agents as most at risk. Lawyers, including solicitors working on real estate transactions, were similarly cited (4%).

Fraud, bribery and corruption need to take place first, before the proceeds are placed in the financial system, layered to disguise the trail, then integrated before big purchases can be made undetected.

When considering who within the financial architecture was most at risk, 15% of fintechs saw corporate and investment banks as being more exposed, while only 7% of respondents from the banking sector believed they were most at risk.

Investment firms and brokers are perceived as a relatively higher risk (cited by all respondents at 11%), although they may also be a transit point in more complex financial manoeuvres. Erik Morgan, managing director of global due diligence at RBC Investor & Treasury Services, a provider of custody, payments, treasury and asset services for institutional investors, agrees that custodians, asset servicers and the investment industry are at risk of structuring or layering of money that has already been laundered.

“Cash or investments into the funds we provide services to originate from individuals or entities via banks, and so there is a risk of receiving laundered funds that have already infiltrated the financial system,” Mr Morgan says.

There is also an international reputational risk for asset services firms like RBC Investor & Treasury Services. According to the Investment Association, 40% of the UK’s £5.7tn worth of investment funds are managed for overseas clients.⁹

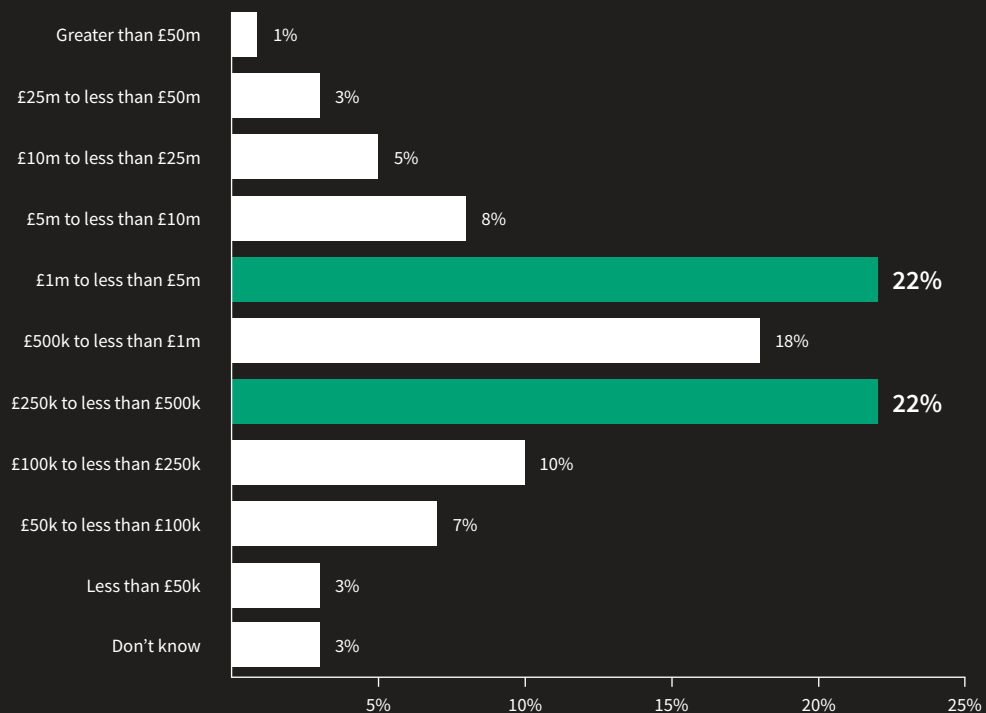
“A rigorous due diligence is required to ensure that no external party looks to use our good name for a veneer of respectability,” adds Mr Morgan.

THE COST OF CRIME

Protecting the country from laundered funds and protecting corporate reputations is costly. The Financial Conduct Authority (FCA) says the businesses it regulates employ at least 11,000 full-time equivalent staff specifically for money laundering and financial crime issues.¹⁰ The salary bill alone is £650m per year.

Yet preventing crime is not just the task of corporate Money Laundering Reporting Officers and internal fraud units; it involves everybody from frontline staff to the CEO. In 2015 the British Bankers’ Association, now part of UK Finance, put the total annual cost of AML at £5bn or more for the banking industry alone—and this excludes fines for AML breaches.¹¹

Figure 3
Total annual cost of overall AML compliance operations (n=204)



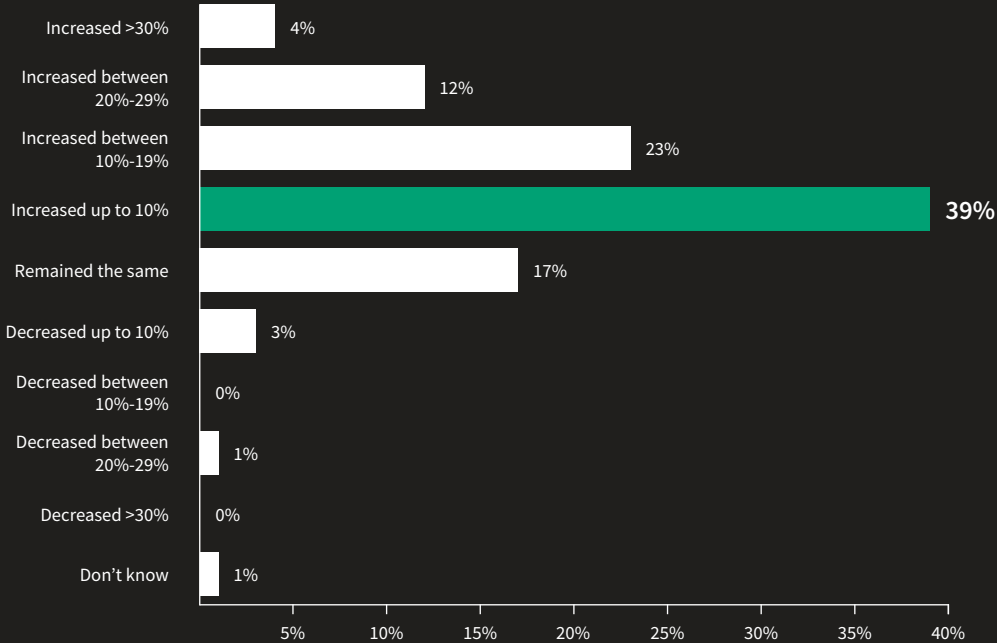
9. UK A Global Investment Hub, The Investment Association, <https://www.theinvestmentassociation.org/assets/files/about-industry/20160922-ukaglobalinvestmenhub.pdf>

10. Financial crime: analysis of firms’ data, Financial Conduct Authority, 13 November, 2018, <https://www.fca.org.uk/publication/research/financial-crime-analysis-firms-data.pdf>

11. BBA response to Cutting Red Tape Review – Effectiveness of the UK’s AML Regime, British Bankers’ Association, 6 November 2015, <https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime/>

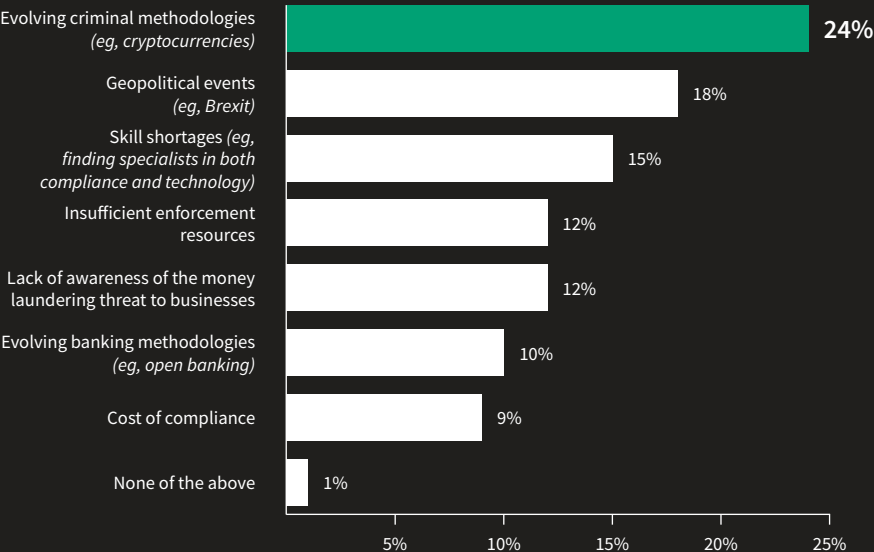
According to 39% of survey respondents, their company is spending £1m or more on AML compliance, with one in six larger banks reportedly spending over £10m.

Figure 4
Change in overall annual cost of AML compliance over past 24 months (n=204)



And, based on recent history, these costs are expected to increase. For 78%, AML compliance costs have increased over the past two years. One in six respondents say compliance costs have risen by more than 20%, rising to more than one in three for those deploying advanced technology.

Figure 5
Single biggest risk to the UK in the fight against money laundering over the next 12 months (n=204)



Costs however, are not the biggest concern for our survey respondents. For 24%, criminal methodologies are getting ever more creative. The law, as well as compliance departments and industry procedures, needs to keep up.

THE BREXIT EFFECT

Despite claims by some politicians and some sections of the media that the EU imposes unwanted rules on the UK, the UK has often steered the direction of AML regulation. The UK has led pan-national regulatory developments and gold-plated the results for domestic use.

However, despite the UK's relatively strong AML record, Brexit creates a challenge. The potential loss of access to European security databases following Brexit means that 18% of respondents have geopolitical concerns. These concerns are felt most keenly by 20% of smaller banks and larger fintechs respondents and 25% of the legal, real estate and gambling industry respondents.

EVOLVING CRIMINAL METHODOLOGIES

Technology is being used by money launderers as well as by those tasked with hunting them. Mr Dilley says accounts opened with forged documents are now less than 1.5% of the total, so criminals now target genuine account holders to launder the proceeds of crime for them. Social media and mobile banking are their tools of choice.

Fraudsters are targeting young bank and card customers via Facebook, Instagram and Snapchat adverts promising "easy cash".¹² Gullible money mules then launder the criminals' transactions quickly to other accounts, or buy Amazon and iTunes vouchers for the launderers, which can be converted into goods or redeemed.

Fraud prevention service Cifas says the number of 14-24 year-olds identified as money mules jumped by 27% in 2017.¹³ And Santander recently told the House of Commons Treasury Committee it closed around 11,000 suspected money mule accounts last year.¹⁴

Given the rise in low-value laundering, such as smurfing (where multiple individuals make multiple transactions with amounts under the reporting threshold) and money mules, as well as associated fraud, all intermediaries are fighting to attract staff with the right experience to identify and prevent these activities. Skills shortages, cited by 15% of respondents, loom relatively large; 29% of larger banks found this a particular challenge. As Mr Dilley notes, "There has been a war for talent as each big money laundering scandal comes around."

12. Revealed: How fraudsters are scamming teenage 'money mules' on Instagram and Snapchat, Sky News, 8 February 2019, <https://news.sky.com/story/revealed-how-fraudsters-are-scamming-teenage-money-mules-on-instagram-and-snapchat-11630666>

13. Fraudscape, Cifas, 18 April 2018, <https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2018>

14. Banks close thousands of 'money mule' accounts, MPs told, The Guardian, 13 February 2019, <https://www.theguardian.com/business/2019/feb/13/banks-close-thousands-of-money-mule-accounts-mps-told>

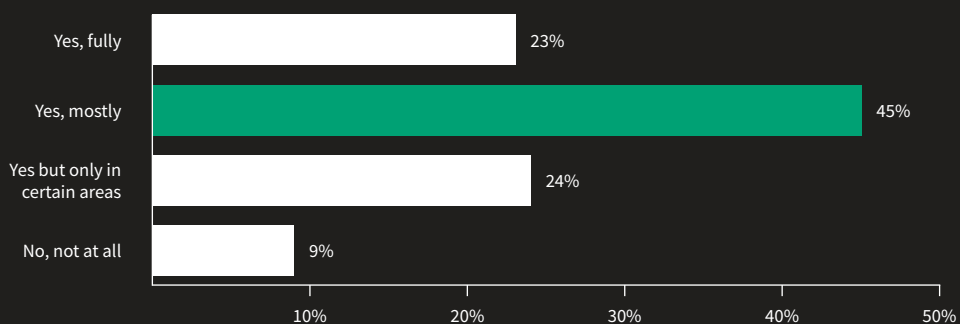


OVER TWO THIRDS OF
SURVEY RESPONDENTS THINK
REGULATORS AND REGULATED
FIRMS ARE DOING ENOUGH TO
TACKLE MONEY LAUNDERING.

CHAPTER 2: THE APPETITE FOR BATTLE

In December 2018 the Financial Action Task Force gave the UK a relatively clean bill of health for the robustness of its AML regime. Economist Intelligence Unit survey respondents would appear to agree: a little more than two-thirds think regulators and regulated firms are doing enough to tackle money laundering.

Figure 6
Is enough being done by the UK regulator and regulated businesses, collectively, to address the money laundering problem in the UK? (n=204)



That perception is strongest among the largest banks, with 76% agreeing compared with only 68% of their smaller competitors (or other intermediaries, ie, gaming, legal, and real estate). Fintechs are the most sceptical of the claim, with around one in eight larger fintechs (those with revenue of more than £500m) thinking the collective effort is not up to scratch.

SUSPICIOUS ACTIVITY REPORTING

Measuring how proactive UK businesses are at rooting out criminals and suspicious transactions is not an exact science. The most comprehensive data come from the SARs that must be sent whenever a regulated business thinks a customer or transaction is amiss.

The quality and quantity of these reports have been heavily criticised by the financial industry, lobby groups, the Law Commission and even the NCA. Data can be incomplete. Transaction-heavy banks and building societies tend to over-report, most likely as a defensive measure against regulatory action. The professional services sector tends to under-report, although just how many SARs should be filed by estate agents, lawyers and others is hard to judge given the nature of the crimes involved.

As Paul Kilbride, chief compliance officer and money laundering reporting officer for Secure Trust Bank notes, the volume of SARs filed has to be taken in context. His bank does not offer current accounts, so it has a low-transaction level relationship with retail customers.

“The volume of SARs submitted to the NCA by the bank is low, which reflects the limited product range, target customer types and scope of products offered. It would be difficult to quantify value being derived directly from the SARs but we understand the overall value as part of a potentially wider investigation,” he says.

Figure 7
SARS: an onslaught of intelligence

Suspicious Activity Reports rose by 9.6% to just under half a million in fiscal year 2017/18. Non-financial firms submitted less than 3% of the total.

APRIL 2017 TO MARCH 2018	VOLUMES	% OF TOTAL
Credit institution – banks	371,522	80.08%
Credit institution – building societies	19,640	4.23%
Credit institution – others	13,678	2.95%
Financial institution - MSBs	21,198	4.57%
Financial institution - others	21,446	4.62%
Accountants and tax advisers	5,140	1.11%
Independent legal professionals	2,660	0.57%
Trust or company service providers	53	0.01%
Estate agents	710	0.15%
High value dealers	249	0.05%
Gaming (including casinos) / Leisure (including some not under Money Laundering Regulations [MLRs])	2,154	0.46%
Not under MLRs	5,488	1.18%
Total	463,938	100%

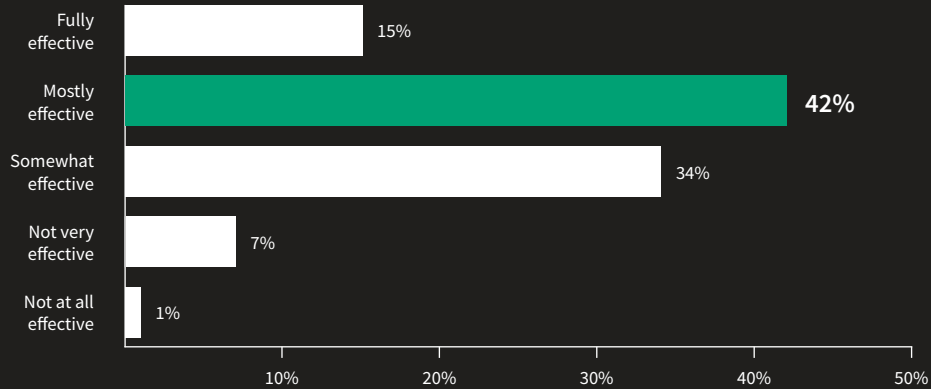
Source: Suspicious Activity Reports (SARs) Annual Report, National Crime Agency, 20 December, 2018

INCONSISTENT EFFECTIVENESS

The majority of respondents (57%) believe the current AML framework is effective at pushing regulated businesses to tackle money laundering, with 60% believing that it is proportionate to the threat their companies face.

Ben Steyn, head of compliance at money remittance fintech giant Transferwise, agrees. To Mr Steyn, the EU’s Fourth Money Laundering Directive (known as 4MLD) and its UK interpretation are a vast improvement on past legislation.

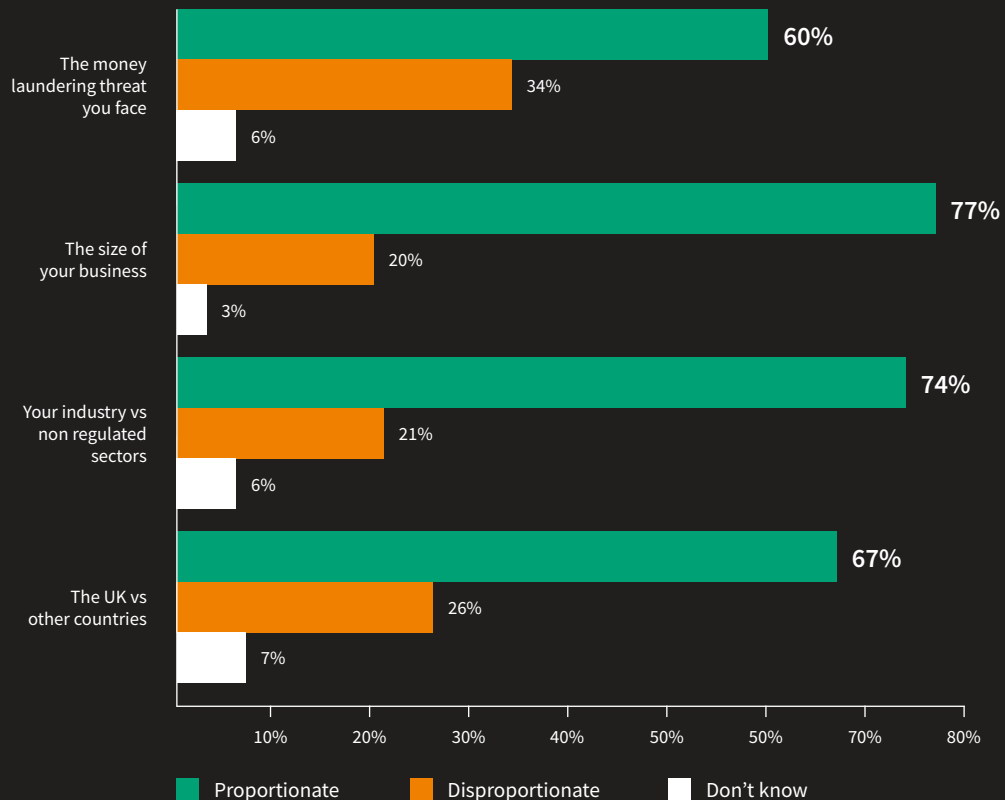
Figure 8
Effectiveness of UK money laundering framework (n=204)



“As a regulatory framework that governs financial crime, it has seen a massive evolution over the course of the last 10 to 15 years. In the early 2000s, money laundering controls were super prescriptive, now they are based on risk,” he says.

Earlier incarnations of the directive were viewed by many regulated entities as too rules-based and rigid, particularly when prescribing how and when regulated firms should verify their customers. As Mr Steyn explains, if criminals know there are additional checks on transactions over €5,000, they simply send smaller sums, rendering the rules virtually useless.

Figure 9
Is the current regulation proportionate or disproportionate to the following: (n=204)



A woman with dark hair and glasses is looking down at a tablet. The tablet screen displays a world map with various data points and icons, a bar chart, and a circular diagram. The background is dark with bokeh light effects.

**THE VIEW ON THE OVERALL
EFFECTIVENESS AND
PROPORTIONALITY TO THE
THREAT FACED BY BUSINESS
IS FAR FROM CONSISTENT.**

But the view on the overall effectiveness and proportionality to the threat faced by business size and industry is far from consistent. Just over half (57%) of respondents think the regulatory framework is at least mostly effective, but not necessarily appropriate for their industry or size. Banks, as the main conduit for payments, are twice as likely to believe efforts are fully effective (22%), than those who work in the fintech and the intermediary sectors.

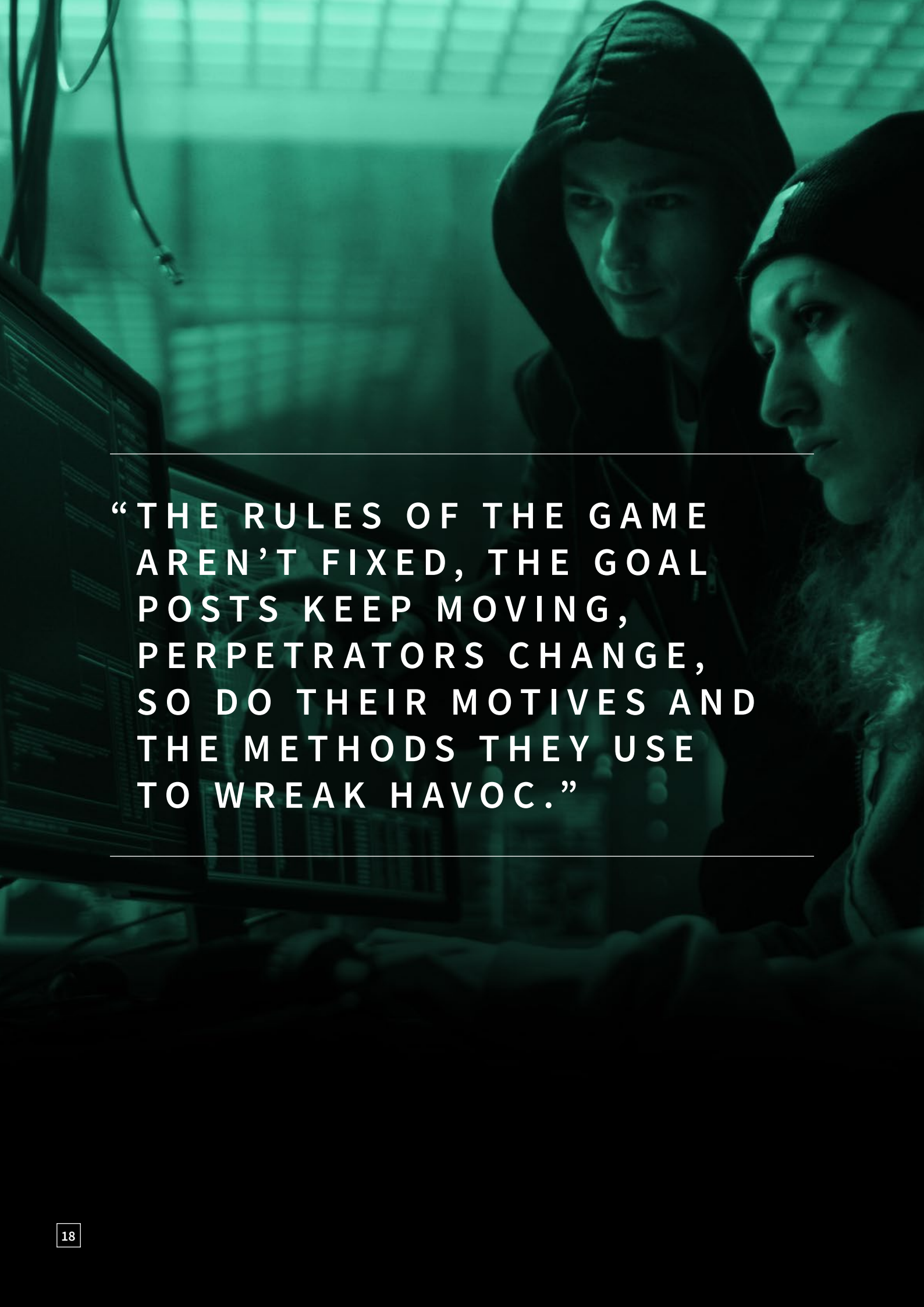
The picture also varies according to the AML technology that businesses are deploying. Of those already using advanced solutions such as artificial intelligence (AI) and machine learning, 73% are most confident about the framework. However, among those lagging to deploy these technologies, the figure drops to 51%.

Secure Trust Bank's Mr Kilbride says AML requirements are proportional for its personal deposits, retail finance and motor loan products, and simple and transparent enough to transpose into operational processes.

"We utilise electronic ID verification tools, which work well with a high pass rate. The challenge is to find a solution that works for those that fail and a manual process is the current default," he says.

The bank has looked at numerous solutions, including customers taking a mobile phone "selfie" photograph with their passport or ID.

"These are not currently the accepted norm in the industry and even though there is appetite to use a solution of this type to improve the customer journey and limit delays, it is unlikely to be introduced in the near future. These types of simple relationships are the majority of our activities and I believe requirements are proportional to the underlying risk," Mr Kilbride says.

A dark, teal-tinted photograph of two individuals wearing hooded sweatshirts, looking intently at a computer monitor in a dimly lit room. The scene suggests a cyber-security or hacking environment.

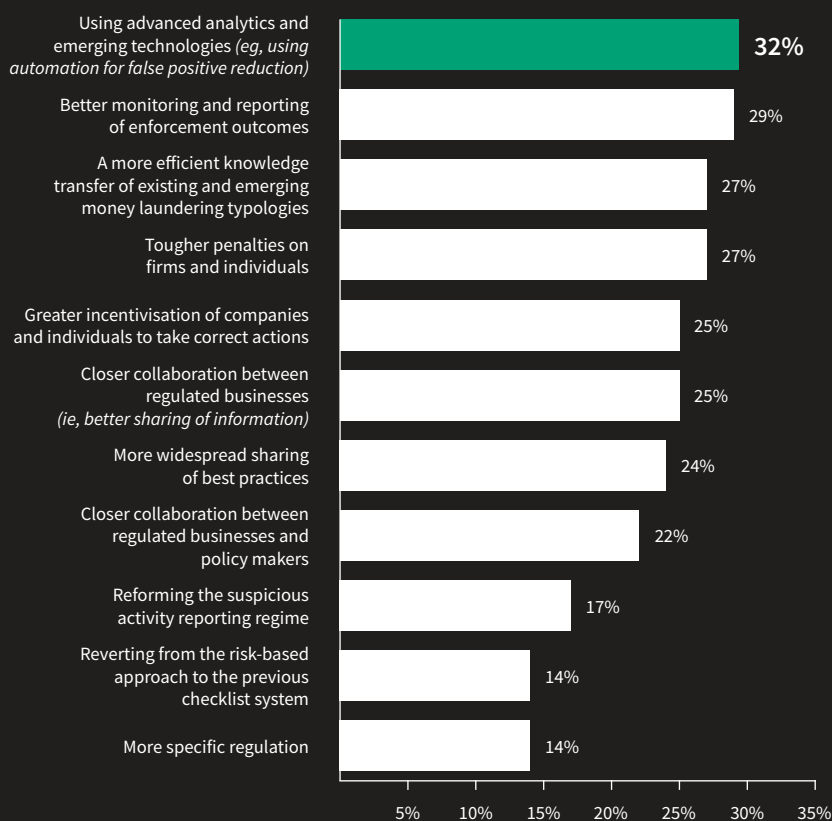
**“THE RULES OF THE GAME
AREN’T FIXED, THE GOAL
POSTS KEEP MOVING,
PERPETRATORS CHANGE,
SO DO THEIR MOTIVES AND
THE METHODS THEY USE
TO WREAK HAVOC.”**

CHAPTER 3: PREPARING FOR COMBAT

When the UK government launched its recent Serious and Organised Crime Strategy, it admitted that tackling financial crime is not getting any easier. The introduction of new technologies makes it far cheaper and easier for all criminals, from the experts to the unskilled, to conduct their activities. The Dark Web, cryptocurrencies, encryption and virtual private networks often render money trails invisible to traditional means of detection.

TECHNOLOGY AMMUNITION

Figure 10
Most effective ways to improve AML. (Respondents could select up to three answers) (n=204)



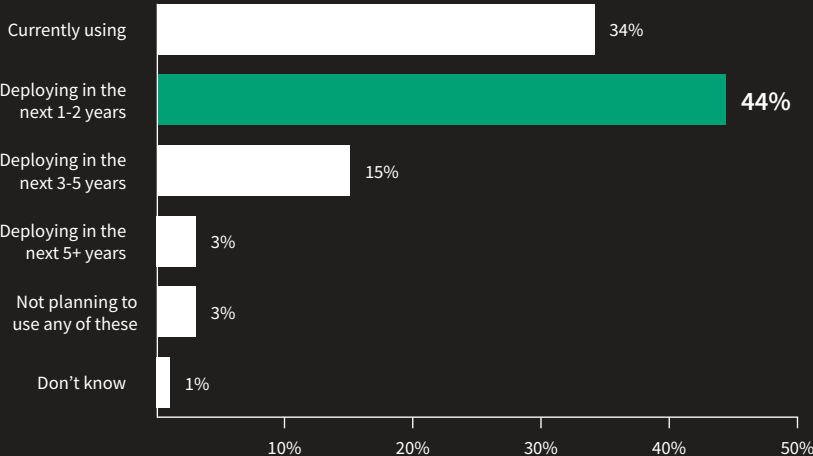
How best, then, to improve the overall approach to tackling money laundering? Survey respondents have plenty of ideas, including a mixture of carrot and stick—with 25% citing the use of incentives to take the correct actions, 24% calling for more widespread sharing of best practice, and 27% calling for tougher penalties for firms and individuals who fail to comply.

Almost a third (32%) of respondents say advanced analytics and emerging technologies can deliver better results. But as Rob Gruppetta, head of the financial crime department at the FCA, admitted in his November 2018 speech, using technology to defeat the criminals is not without its own constraints.

For example, AI and machine learning rely heavily on data from past transactions to calculate what might happen next; for those without the critical mass this will prove challenging. And as criminal methodologies change, tech needs to keep up.

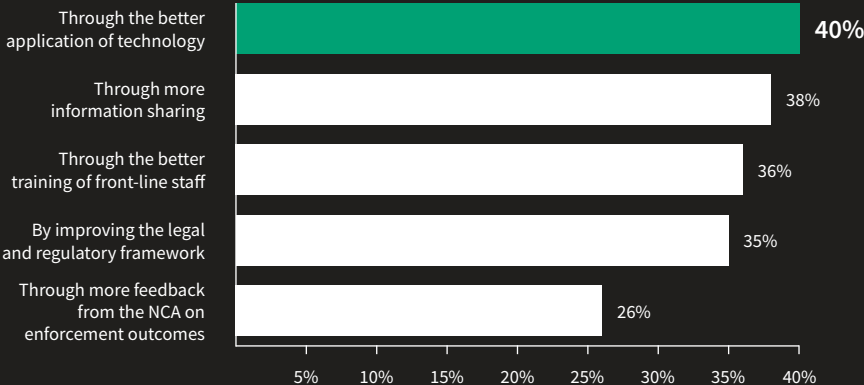
“The rules of the game aren’t fixed, the goal posts keep moving, perpetrators change, so do their motives and the methods they use to wreak havoc,” said Mr Gruppetta. In a dynamic and uncertain environment, a static algorithm is not going to be of much use.

Figure 11
Use of advanced analytics/AI/machine learning for AML (n=204)



When it comes to deploying advanced technologies, 40% of banks and 37% of larger fintechs are doing so, compared with 34% across all regulated sectors. A further 40% of banks and 60% of large fintechs plan to introduce these within the next two years.

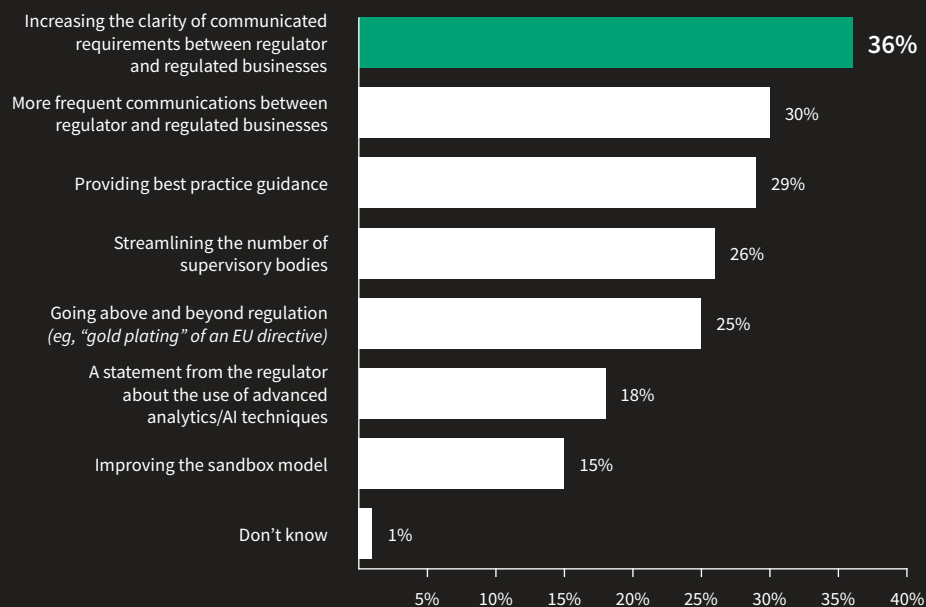
Figure 12
How to improve the SAR process. (Respondents could select up to two answers) (n=204)



Technology is seen by 40% of respondents as the key to improving the SARs regime itself. But tech for tech's sake is not enough; as noted by 36% of respondents, frontline staff need training on how to spot suspicious customers and behaviour, and 38% agreed that information must be shared more effectively. More than one in every four respondents (26%) wants more feedback from the NCA on what enforcement actions are taken based on their SAR submissions.

JOINING FORCES

Figure 13
Which regulatory initiative do you believe would most improve the efficiency of AML compliance in the UK? (Respondents could select up to two answers) (n=204)

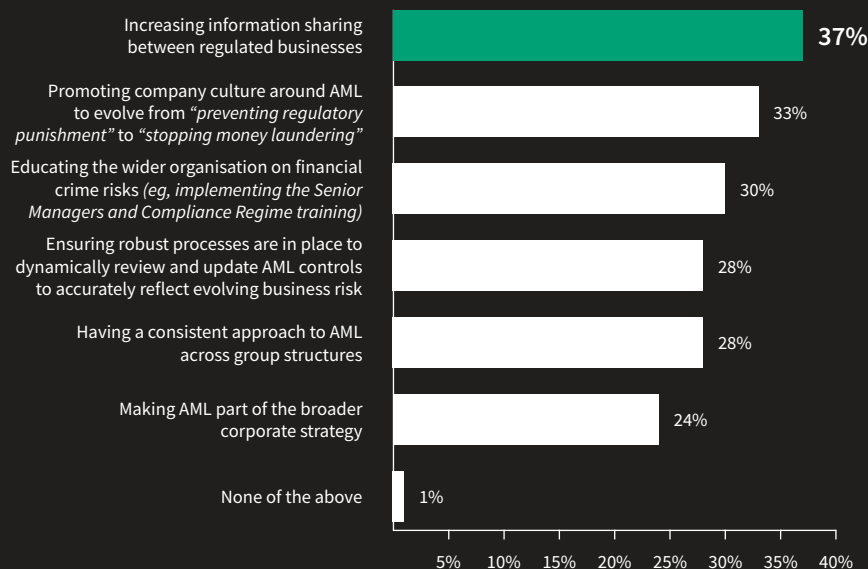


From a regulatory perspective, 36% of respondents want to see more clearly communicated requirements and 30% want more frequent guidance from authorities. And 29% want more guidance when it comes to best practice. This was especially the case for smaller fintechs (42%).

For 29% (Fig 10) of respondents, better reporting of enforcement outcomes would be useful. Most interviewees agreed that their firms need more feedback on what their reports and data sharing actually achieve in terms of arrests and seizure of assets.

However, respondents are not calling for a complete overhaul of the regulatory environment, as only 14% (Fig 10) want to return to the rigid checklist methods of the past.

Figure 14
 How could companies better combat money laundering? (Respondents could select up to two answers) (n=204)



From a corporate point of view, the sharing of information between regulated firms was viewed as the most useful approach by 37%. That view is most heavily held by the gaming, legal and real-estate sectors (cited by 43% in those sectors).

The Joint Money Laundering Intelligence Taskforce (JMLIT) has been bringing together the police, prosecution agencies, regulators and financial services firms since 2015. The JMLIT aims to understand the funding flows linked to bribery, corruption, money laundering, human trafficking, modern slavery and terrorism financing, sharing that information with vetted staff from a range of banks.

Although this may be viewed as a step in the right direction, it has had a limited effect. This is because it does not include intermediaries outside of a select number of banks and the law does not yet allow full and frank co-operation.

Frustrations arise as banks, wishing to notify their peers, cannot share information about an individual, account or transactions until the threshold of “suspicion” has been met, at which point they are compelled to submit a SAR.

“There are limitations on what we can do. The Criminal Finances Act didn’t give us the ability we were asking for to discuss things below suspicion with other institutions,” says Lloyds’ Mr Dilley.

This often reduces the system’s ability to be proactive. If banks could share more, and earlier, the picture that SARs paint could be richer in detail. The question for many may be, what about the General Data Protection Directive (GDPR)? There are allowances in GDPR on using customer information in the fight against financial crime with proper controls and safeguards in place. However, if a situation arises where financial institutions share data for compliance purposes, banks need to be mindful of confidentiality obligations.

Lloyds Banking Group is working on a proof of concept that would allow each participant institution to anonymise or hash information that is then placed in a central pool for others to view. This could allow AML teams to look at groups of transactions across multiple institutions and accounts, rather than only looking at transactions solely within their own bank.

THE WILL TO FIGHT

Yet changes to regulation alone will not ensure greater internal or external collaboration. Corporate culture counts for a lot and direction should come from the top. A third (33%) of survey respondents agreed that mere compliance to avoid fines is not enough: companies must want to end money laundering altogether.

Transferwise's Mr Steyn also senses internal resistance to change across the regulated sectors. He believes there is a lingering industry view that verifying a customer face-to-face is more secure than using online processes.

"We strongly disagree with that. Regardless of the speed, we still have so many more touch points with the customer that form part of their online footprint than when you're using cash. Online identity is far more than a passport copy or a utility bill," he says.

In this digital era, all customers want speed and convenience. It therefore falls to the regulators, enforcement agencies and regulated firms to find the right balance to achieve customer satisfaction without compromising the ongoing fight against financial crime.

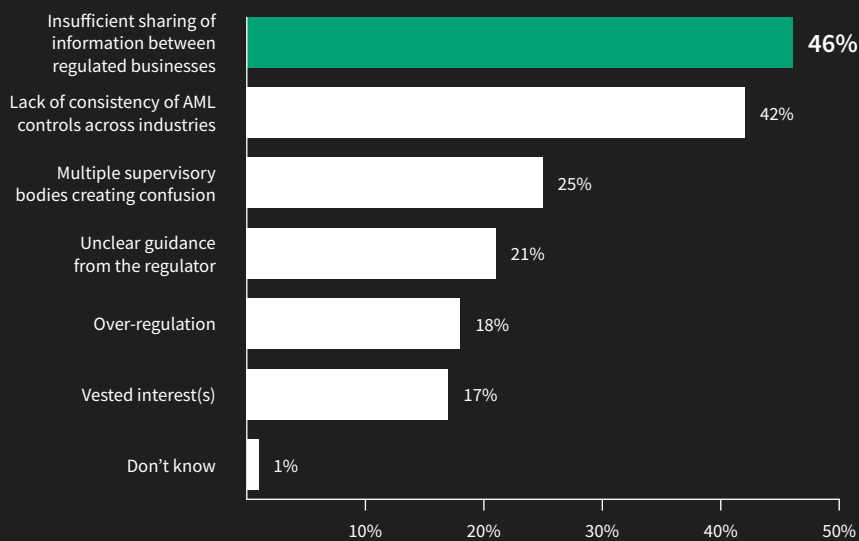


**THE BIGGEST BARRIER
REMAINS THE LACK OF
INFORMATION SHARING
BETWEEN REGULATED
BUSINESSES.**

CHAPTER 4: CLEARING THE OBSTACLES

There are numerous reasons to think that there is room for improvement to the AML regime and procedures. What emerges from the survey is that regulatory guidance needs to be clearer if authorities expect firms to comply effectively.

Figure 15
Biggest external barriers to efficient AML. (Respondents could select up to two answers) (n=204)



The survey reveals that one of the biggest external barriers to efficient AML, cited by 25% of respondents, are the multiple regulators that oversee how rules are implemented. The biggest barrier (46%) remains the lack of information sharing between regulated businesses, followed by inconsistent controls being applied across the various sectors (42%).

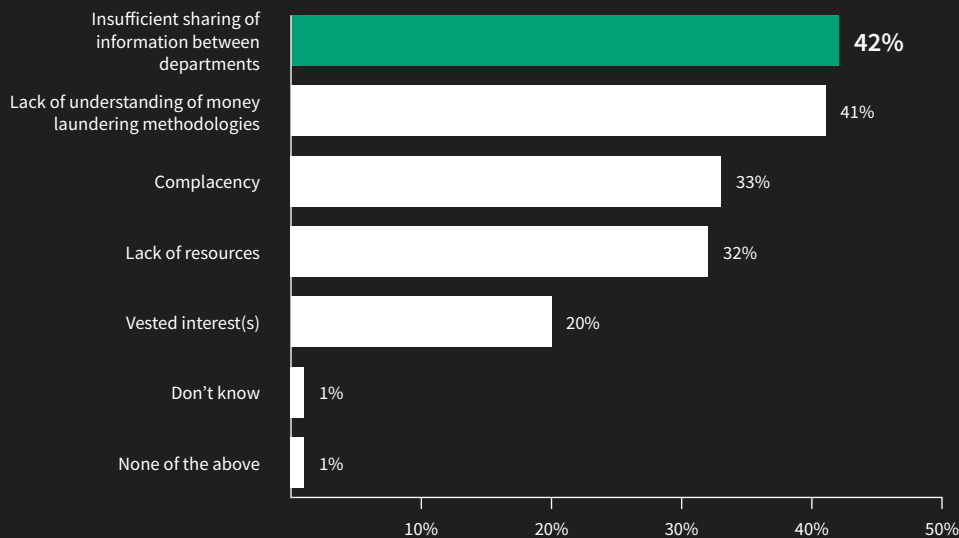
WHO IS IN CHARGE?

When the EU's Fourth AML Directive was adopted into UK law, many professions had little time to adjust, with the consultation lasting just weeks and the new laws coming into force two months later. Twenty-two professional bodies are charged with ensuring insolvency practitioners, lawyers and even notaries licenced by the Archbishop of Canterbury abide by the rules.

In an attempt to ensure consistent standards are applied across such professional bodies, a new Office for Professional Body Anti-Money Laundering Supervision (OPBAS) is pushing for best practices. It has much to do. Indeed, respondents from the gaming, legal and real-estate sectors (23%) are still most likely to feel that regulatory guidance is lacking.

12 months on from its inception, the OPBAS said 80% of Professional Body Supervisors in the legal and accountancy sectors lacked appropriate governance and nearly half lacked clear accountability and oversight for AML supervision at a senior level.¹⁵

Figure 16
Biggest internal barriers to efficient AML. (Respondents could select up to two answers) (n=204)



15. Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Themes from the 2018 OPBAS anti-money laundering supervisory assessment, Financial Conduct Authority, 12 March 2019, <https://www.fca.org.uk/publication/opbas/themes-2018-opbas-anti-money-laundering-supervisory-assessments.pdf>

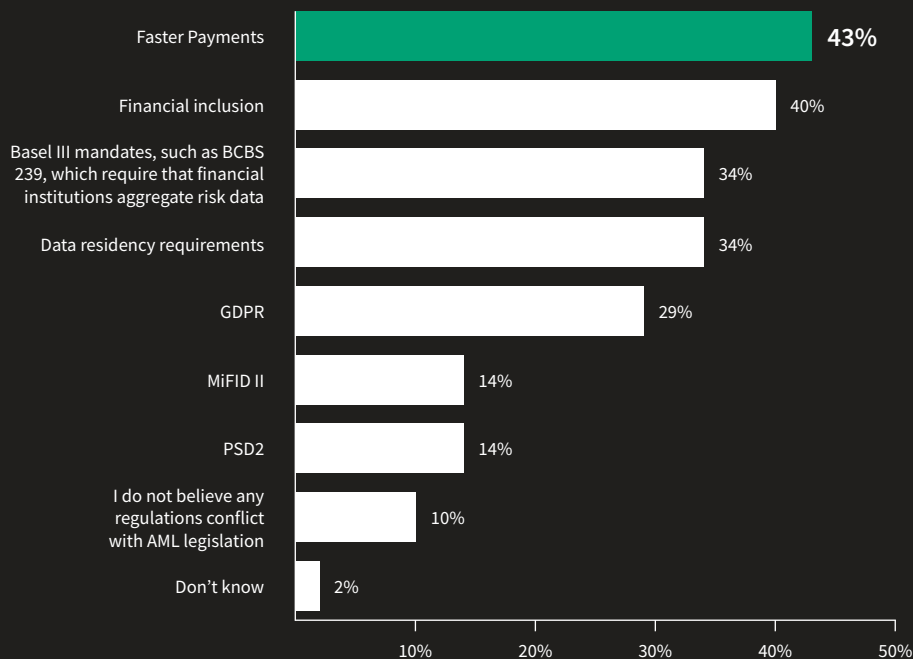
If external information sharing needs improving, internal sharing (42%), fares only a little better. Those most likely to think there is insufficient sharing of information are finance departments (50%) and advanced technology users (56%). These barriers are reinforced by a lack of workforce understanding of money laundering methodologies (cited by 41%) and complacency (33%).

There are bright spots, however. As Mr Dilley of Lloyds suggests, the banking industry is seen as leading collaboration and consistency: “Within the banking industry, comparatively, collaboration is far better.” In other sectors, practices are often ten years behind the banks, even in basic Know Your Customer (KYC) documentation requirements, although the situation is now improving, he notes.

CONFLICTING REGULATION


AML rules do not operate in a vacuum. They must interact with other laws that keep the financial system operating, both domestically and internationally.

Figure 17
Regulations conflicting with AML. (Respondents could select up to two answers) (n=204)



“The inherent risks associated with cross-border payment and correspondent banking are naturally high,” admits Mr Morgan at RBC Investor & Treasury Services.

“Anti-money laundering regulations shouldn’t conflict [with other regulation], but sometimes due to the challenges around subjectivity of interpretation and different rules in different jurisdictions, they might,” he says.

A man in a white shirt is sitting at a desk in an office, talking on a mobile phone. He is holding a pen over a notebook. On the desk, there is a laptop, a coffee cup, and a pair of glasses. The background shows office windows and lights. The entire image has a teal/green color overlay.

“COMMUNICATION BETWEEN BANKS AND OTHER BODIES THAT MANAGE FUNDS IS VERY DIFFICULT. THAT SHOULD BE MADE EASIER USING TECHNOLOGY.”

New regulations to make life simpler for financial customers often cause problems too. Historically, payer and payee banks had three whole days to check a suspicious cheque before cleared funds could be spent or withdrawn. In the online and mobile world of Faster Payments and its European equivalent, the Single Euro Payment Area's Instant Credit Transfer, they now have fractions of a second.

Therefore it is not surprising that 43% of respondents think the Faster Payments rules conflict with existing AML legislation. And if payment firms struggle to keep up, their customers often do too. UK enforcement agencies have seen an unprecedented rise in push payment fraud; this is where hackers convince unwitting account holders to direct money to laundering accounts. This is done by tricking consumers or individuals in a business into making a payment, or by intercepting an email chain and changing the payment information, when, for example, completing a house purchase. Once the payment is made, the money is quickly moved, making it harder to trace and reclaim.

When it comes to speed, Monzo, a mobile-only bank launched in 2015, is not keen on any deliberate brakes being introduced into the Faster Payment system. But there are improvements that can be made to ensure fraudulent payments can be traced and fewer genuine customers are scammed, if only the banks would agree.

“Communication between banks and other bodies that manage funds is very difficult,” says Natasha Vernier, head of financial crime at Monzo. “That should be made easier using technology.”

It does not help that basic security checks on the recipients of payments are not being implemented as quickly as they should be. A new Confirmation of Payee system, designed to match the recipient name entered by the sender to the actual name of the recipient account holder, has been delayed until next year.¹⁶ As a new, technology-focused bank, Monzo says it is already testing these checks; traditional banks have said they will miss the original summer 2019 deadline.

Other regulations like MiFID II rules, which cover transparency in investments in equities, bonds and investment funds, are seen as less of a conflict (14%). This may change as global regulators tackle market manipulation. Moreover, the ramifications of the Panama and Paradise Papers leaks, which highlighted the complicated webs of domiciles and untraceable investment vehicles used to shunt money around the world, are still to be fully felt.

16. Name checks on payments face delay, BBC News, 14 February 2019, <https://www.bbc.co.uk/news/business-47231337>

TALENT WAR

Technology has changed the AML landscape, but the bulk of AML compliance budgets are still spent on human beings. Headcount takes up 33% of the budget, with a further 29% allocated to training employees directly in the AML function and throughout the rest of the business.

Figure 18
Distribution of AML compliance costs (n=204)

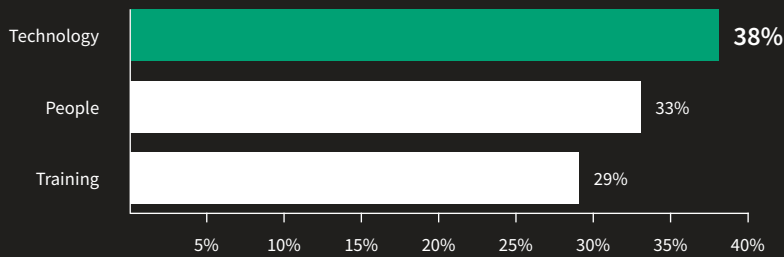
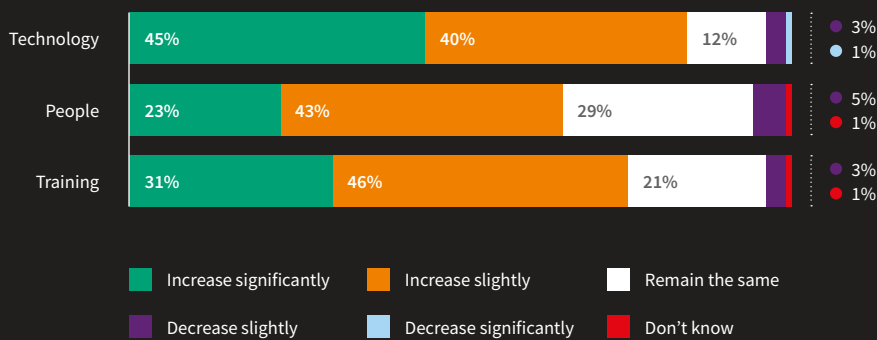


Figure 19
Evolution of AML costs over next 3-5 years (n=204)



The majority of respondents see costs for both human elements increasing, with a particular focus on training (77%), while staff costs are predicted to rise for 66% of respondents. The human element is also a big concern (76%) for those already using new technologies. This reinforces the message that technology alone is not sufficient, and pressure on salaries will continue for some time, with regional differences across the country.

Regulated firms outside of the main financial hubs of London, Bristol and Edinburgh, may find that staff are lured away by higher salaries.

“Demand is strong for experienced and quality professionals in the industry and is a challenge in the location of the head office with strong local competition,” says Mr Kilbride at Secure Trust Bank, based in the West Midlands.

Technology costs are also expected to rise (85%), a view almost universally shared by fintechs (89%) and those already deploying advanced technologies (90%).

Transferwise's Mr Steyn points out that there is a definite correlation between growth in the business, financial crime and its crime-tracking resources. The balance between reporting staff and machines could change in favour of the latter, as technology allows the firm to spot more data points and build its capability in link analysis, a process that analyses connections between different nodes (such as a mobile phone and a set of accounts).

The challenge for Transferwise now is one of scale. Its financial crime team that handles verification, enhanced due diligence and AML has grown to 15% of its staff base. Mr Steyn says the company needs to build its accumulated knowledge back into its automated systems if it is to maintain its growth and generate profits.

THE INDISPENSABLE HUMAN TOUCH

There are also products, services and procedures that may not be suitable for full automation. An example of this is Secure Trust Bank, which has to rely on face-to-face contact in its real estate and commercial finance, especially when it comes to identifying ultimate beneficial owners (UBOs) for businesses.


"When the structures can occasionally be complex and include overseas UBOs, these can be time consuming to fully extract the required information to the required standard, but management understand the need to ensure this is so. There is no obvious tool available to avoid the lengthy back office processes to conduct the full end-to-end verification of the individuals in the structure," says Mr Kilbride.

Lloyds' Mr Dille has a simple explanation as to why the users of advanced technology may also see their human and IT costs rising faster—they may be going above and beyond what the law requires of them.

"The AML regime has not kept pace with the move into the digital world. If you look at what we're doing, it is not just KYC, we are monitoring all sorts of behavioural characteristics, such as the way people use their devices, and the device characteristics themselves," he says.

Lloyds, which includes the Bank of Scotland, Halifax and Scottish Widows brands, is investing in technology to monitor customer behaviour. This may involve looking for accounts controlled from the same mobile device, or accounts that share common voiceprints, even if they are registered in different names.

As Mr Dille notes, underlying transactions may appear normal, especially if criminals know what the banks are looking for. However, when IP addresses, mobile numbers and biometrics are combined, the patterns will be easier to spot.



TECHNOLOGY IS A VITAL TOOL, PARTICULARLY IN A WORLD OF FAST PAYMENTS. NEWLY REGULATED SECTORS SHOULD RAMP UP THEIR KYC AND TRANSACTION MONITORING PROCEDURES TO FULLY EMBRACE THE DIGITAL AGE.

CONCLUSION: COMMUNICATE, CO-OPERATE

Over two-thirds (67%) of regulated firms in the UK believe the current AML regime is proportionate when compared with efforts in other countries. They are also highly aware that more needs to be and can be done to stop the billions of pounds derived from fraud, bribery, human trafficking and drug running being laundered in the UK.

Technology is a vital tool, particularly in a world of fast payments. Newly regulated sectors should ramp up their KYC and transaction monitoring procedures to fully embrace the digital age.

Although such technology can aid reporting by automatically flagging behaviour worthy of a SARs report, people and collaboration are even more important. The survey and interviews strongly indicate three key trends:

1. An ongoing battle for AML talent;
2. A desperate need for more information sharing within and between sectors;
3. A greater need for more information sharing with the NCA, the FCA and other enforcement agencies.

Our survey shows that regulated industries clearly want to be more proactive, but they are often restrained by a raft of regulations and procedures like data residency rules and GDPR.

And it is not just the private sector that recognises the need for change. Both business and politicians will be looking to the new Economic Crime Strategic Board, launched in January 2019, to provide much needed reform to the SARs system. This board, with its £3.5m budget, and hosted by the Home Secretary and Chancellor of the Exchequer, brings together banking leaders, other regulated sectors and crime agencies.

Whatever the board decides, it is clear that the government and private sectors may have to adopt a longer term approach to AML, including a commitment of not only more financial, technological and human resources, but also a change of mindset. Money laundering is an ever evolving crime, and therefore the battle against it requires an ever evolving approach.

APPENDIX

THE SURVEY

The survey included 204 senior compliance, finance and legal executives from regulated industries at the centre of the fight against money laundering. These included members of the banking industry, financial technology sector, legal professions, real estate sector, and gaming and gambling industries.

- Forty-one percent of respondents come from the banking industry, with an even split between small banks (with revenues under £1bn per year) and larger competitors (with revenues over £1bn per year).
- A further 30% are in the fintech sector, reflecting the importance of new challenger banks, pre-paid card providers and neo-banks that offer banking facilities without the need for a deposit account, and providers of tech services.
- The remainder (29%) are split between the legal profession, real estate, and gaming and gambling—all industries facing greater scrutiny in the fight against money laundering.
- By function, finance, compliance and legal professionals dominated the survey base. Over a third are C-suite executives (29%) or higher (managing director 9%) in their organisation's structure. Nearly all (97%) have or share direct responsibility for monitoring compliance with AML regulations.

REMEMBER WHAT
WE'RE FIGHTING FOR

For more information, call 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk



About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers across industries. For more information, please visit risk.lexisnexis.co.uk and www.relx.com.

The paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. The report does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their legal advisors, compliance departments and other professional advisors about any questions they may have as to the subject matter of this paper. LexisNexis Risk Solutions shall not be liable for any losses incurred, howsoever caused, as a result of actions taken upon reliance of the contents of this paper. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. No part of this document may be reproduced without the express permission of LexisNexis. LexisNexis Risk Solutions UK Ltd is a company registered in England & Wales at 1st Floor, 80 Moorbridge Road, Maidenhead, Berkshire SL6 8BW. Registration number 07416642. Tracesmart Limited is a LexisNexis company, operating under the trading name of LexisNexis, with an England & Wales Registration Number 3827062. Registered Office is Global Reach, Dunleavy Drive, Cardiff CF11 0SN. Authorised and regulated by the Financial Conduct Authority (Firm Reference number 742551). Copyright © 2019 LexisNexis. 307/MK/WP/1. NXR13845-00-0519-EN-UK