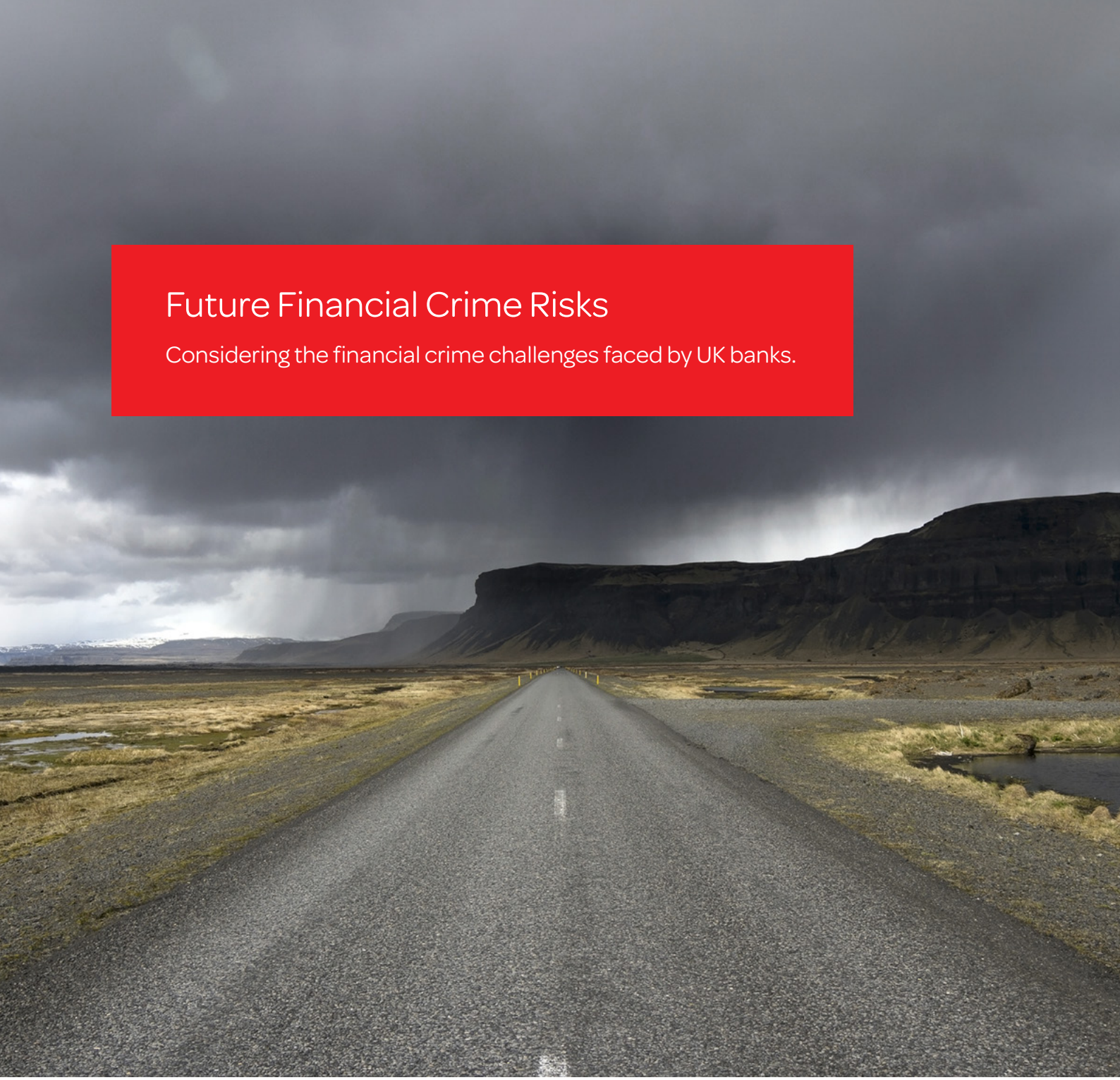


Future Financial Crime Risks

Considering the financial crime challenges faced by UK banks.

A LexisNexis® Risk Solutions report produced for the British Bankers' Association

November 2015

LexisNexis® RISK SOLUTIONS

bba The voice of banking

Table of contents

Executive summary

British banks are on the front line in the battle against financial crime. Both the nature of their business and regulatory design have positioned them as the first line of defence against money laundering, terrorism funding, and an expanding array of other illicit activities.

It is a responsibility that banks - and particularly their compliance functions - take seriously. The size of the potential penalties for failing to uphold their duties is motivation enough. Those who dedicate their careers to tackling financial crime understandably lay claim to a higher motive: a desire to see their banks play an active role, along with regulators and law enforcement agencies, in detecting and preventing financial crime and thereby reducing its impact on society.

Speaking to such people, however, reveals genuine fears about the ability of banks to continue to perform this function in the future.

These fears are based on not just uncertainty over the new risks that may emerge in the future – although we can begin to make educated guesses what these may be – but also problems we can identify today with potential consequences that may become much more serious over time. This report identifies four key trends that will shape banks' response to financial crime in the years ahead, and determine their success or otherwise:

- **The growth in the regulatory burden of anti-money laundering, counter-terrorism, anti-bribery and corruption, and other financial crime regulation (all referred to as AML from here on).** Well-intentioned, but often poorly targeted, we too frequently see "compliance for compliance's sake" as one professional puts it. We are close to a tipping point, with the sustainability of the current approach seriously questioned by many within the industry. In a survey of 198 banking and other financial services compliance and financial crime professionals (Appendix), 61 per cent said there was enough or too much regulation, but inadequate enforcement.

- **Increased personal liabilities for compliance failures, including even custodial sentences for those in banks charged with tackling financial crime.** Effectively imposing on compliance staff the risks and responsibilities of the most senior management, but not the rewards, threatens to undermine the attractiveness of compliance roles. Our survey found that more than half (54 per cent) of compliance professionals would choose another career path if the opportunity arose in light of the increased personal liabilities.

- **The moves and barriers to greater collaboration between and within banks, regulators and law enforcement.** With the potential to make AML efforts more effective and efficient, collaboration has great potential to help face up to the financial crime challenges of the future. However, whilst we are seeing progress with forums such as the Joint Money Laundering Intelligence Taskforce (JMLIT), there are still many barriers – perceived and real – which are inhibiting across the board collaboration.

- **The pace of change in terms of technology, product innovation and criminal methodologies.** Virtual currencies, peer-to-peer financial solutions, mobile payments – all present challenges for compliance, opportunities for criminals and longer term perhaps even existential questions for banks if they cannot find ways to respond and manage the risks. Changing criminal methodologies, including the move to digital technologies is by far the single biggest worry among compliance professionals, the survey found.

Each trend is complex, and will have wide-ranging impacts on the fight against financial crime and banks' ability to be effective participants in it. However, they are also somewhat all inter-related, and two effects are consistently seen across these trends: one is a relentless increase in the cost of banks AML efforts; the other is the threat of undermining the ability to combat financial crime and even adding to and creating new risks.

This report makes it clear that financial crime cannot be eradicated by throwing money at it, and that efforts to combat it based on limited understanding and knowledge of the industry and risks will exacerbate the problem in the future. It is to help develop that knowledge and prevent this from happening that this report has been thoroughly researched, analysed and written. If we can understand the risks of the future, we can perhaps prevent them from materialising.

Introduction

There is no way to measure the full costs of financial crime. Those who commit it have been described as the modern-day equivalents of con-artist Victor Lustig[1], "the man who sold the Eiffel Tower". However, the damage wreaked by today's money launderers, terrorism funders, cyber criminals and those involved in bribery, corruption and fraud, is much greater than anything Lustig managed.

Money-laundering, particularly, is an "enabling crime"[2], facilitating organised crime (as well as terrorism) with social and economic costs to the UK estimated to be at least £24 billion a year.[3] It supports, among other crimes, drugs, people and firearms trafficking, organised illegal immigration, large-scale and high-volume fraud and other financial crimes, counterfeit goods (including medicines), organised acquisitive crime and cyber crime.[4]

Far from being victimless, financial crime costs lives, wrecks communities, reduces trust and undermines national security. Its economic impact worldwide is, likewise, substantial.

As Min Zhu, Deputy Managing Director of the International Monetary Fund (IMF) said: "Money laundering and the financing of terrorism are financial crimes with economic effects. They can threaten the stability of a country's financial sector or its external stability more generally. Effective anti-money laundering (AML) processes and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse. Action to prevent and combat money laundering and terrorist financing thus responds not only to a moral imperative, but also to an economic need."[5]

In reality, and long acknowledged, data on money laundering is poor.[6] Likewise with cyber crime, the biggest challenge is often to establish its true scale.[7] What is clear is that, as a major economy and a global financial centre, the UK is a key battleground from a domestic and international perspective, as the UK government's recent national risk assessment (NRA) of the threat of money laundering has pointed out.[8] UK banks are on the front line.

The National Crime Agency (NCA) estimates that hundreds of billions of pounds are laundered through UK banks each year.

"[I]t will include the proceeds of virtually all serious and organised crime in the UK as well as the proceeds of a significant amount of international serious and organised crime, including corrupt politically exposed persons (PEPs) seeking to launder the proceeds of their corruption and hide stolen assets in the UK," it notes.[9]

The NCA estimate is difficult to verify. In 2007, the UK Treasury estimated money laundering through the entire regulated sector at just £10 billion a year.[10] However, the regulatory focus on financial crime is more difficult to dispute.

1. http://www.fca.org.uk/news/speeches/the-changing-face-of-financial-crime
2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116653/future-organised-crime-res-2011.pdf
3. https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs
4. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf
5. http://www.imf.org/external/np/exr/facts/aml.htm
6. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116653/future-organised-crime-res-2011.pdf *(ibid)*
7. http://www.ft.com/cms/s/0/2504334e-6e51-11e4-bffb-00144feabdc0.html#axzz3od1wX12R
8. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf
9. http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file
10. http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf

Earlier this year the UK regulator, the Financial Conduct Authority (FCA), added financial crime as a key focus, replacing rapid house price growth in its list of top risks.[11] In particular, it vowed to focus on firms' systems and controls in preventing financial crime.

"Firms that fail to place adequate emphasis on implementing necessary systems and controls are more vulnerable to being used to further financial crime," it correctly notes.

The systems and controls necessary, however, and the emphasis required, depend on the nature of the risks, and this – as the FCA notes[12] – changes with time.

This report therefore seeks to understand how these risks are evolving, the consequences of the regulatory regime designed to mitigate them, and what the future of financial crime may look like. To do so, we've spoken to senior law enforcement agents, industry subject matter experts and those in the banks themselves responsible for AML, combating the financing of terrorism (CFT), and controls to combat fraud, tax evasion and other financial crimes. We also conducted a wider survey on some of the key issues these conversations raised, the findings of which we also share throughout this report.

We hope this report helps add to the body of knowledge on money laundering and contributes to a debate that will ultimately make the UK a safer and more prosperous place.

1. A tipping point: the compliance burden

If banks are on the front line of the fight against financial crime, it follows that the regulatory environment they operate in will have a profound effect on its nature and scale – for better or worse.

Even an effective regulatory and enforcement regime will not only mitigate the risk, but also shape its nature going forward, as criminals revise their attacks in response. A poorly targeted approach will, likewise, open up new vulnerabilities, but also be ineffective against, and possibly even worsen, the existing risks. Unfortunately, there is significant support for proposition that this describes the current regime.

"There is substantial skepticism about the efficacy of global systems and national regimes to control money laundering and the financing of terrorism," noted a 2014 report from a study supported by the IMF.[13] An earlier estimate by two of the same authors put the level of seizures by regulators and law enforcement bodies below one per cent of the sums of money laundered[14] each year.

Doubts regarding the effectiveness of the current regime are widespread among banks – and strongly felt. As one director of investigations in compliance at a major bank puts it in an interview with us: "You just end up despairing and asking whether the regulators actually know what they are talking about. Have they got, not just an appreciation of the risk in the first place, but a sense of the controls that can really make a difference?"

11. http://fca.org.uk/static/channel-page/business-plan/business-plan-2015-16.html
12. "It is the nature of predictions that not all of these [risks] will crystallise during the next 12 months and that other priorities will rapidly move up the agenda." *(ibid)*
13. http://www.lexglobal.org/files/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf
14. http://www.bloomberg.com/news/articles/2015-02-23/why-the-world-is-so-bad-at-tracking-dirty-money

1.1 Increasing costs

If controls are ineffective, it is not for want of trying. The costs of compliance failures have consistently grown in recent years. In 2014 alone, the FCA issued almost £1.5 billion in fines.[15] Internationally, fines for AML, sanctions and tax avoidance violations at 20 of the world's biggest banks have totalled more than $17.5 billion in the last seven years.[16]

The impact of such fines is also wider than the individual firms penalised.

"The more a bank gets fined, the more cautious they become. So if a bank is seriously fined and they're your correspondent, the impact is not just on that bank; it knocks anybody who deals with that bank," says one interviewee at a smaller UK bank.

At the same time, and related to this issue, compliance costs have soared. AML compliance costs are estimated to have increased by half in the last three years alone[17], with costs focused on transaction monitoring systems, Know Your Customer systems, and recruitment and retention of AML staff.[18] Our research suggests most major international banks are spending between £700m and £1bn annually on financial crime compliance.

A number of factors have contributed to this position in addition to the increasing penalties for failures. One is simply the scale of regulation, with compliance officers constantly bombarded with regulatory advice, updates and alerts. This is partly down to the number of regulatory agencies – a complaint of not just the banks.

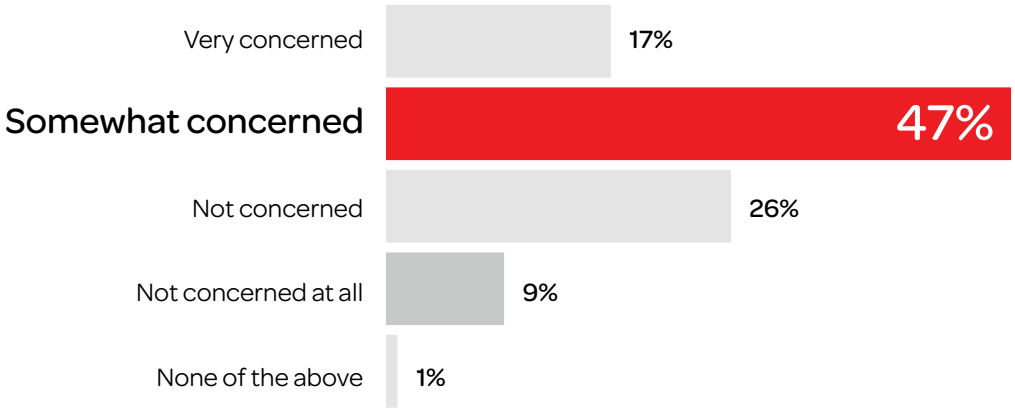
"Have fewer regulators. We have 28 in the UK – far too many," says one senior law enforcement officer we interviewed in answer to the question of how we can make financial crime regulation more effective.

The NRA, too, accepted that "[t]he large number of professional body supervisors in some sectors risks inconsistencies of approach"[19]. Moreover, the exact regulatory status of guidelines, recommendations or principles issued by a range of bodies, from the Bank of International Settlements[20] to the Wolfsberg Group[21], (or the regulatory expectations relating to them) is often unclear to those tasked with compliance.

At the same time, the scope and complexity of financial crime regulation has increased. Banks' responsibilities have been expanded into new areas such as tackling tax evasion, notably through the US Foreign Account Tax Compliance Act[22] (and, looking forward, the Common Reporting Standard), and immigration, through the Immigration Act 2014. Our survey found that the impact of tax evasion over the next couple of years was a concern for almost two-thirds (64 per cent) of those questioned; 17 per cent said they were "very concerned" (See Figure 1).

15. https://www.fca.org.uk/firms/being-regulated/enforcement/fines/2014
16. http://graphics.thomsonreuters.com/15/bankfines/index.html?utm_source=twitter
17. https://www.accenture.com/t20150825T104327__w__/bw-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_20/Accenture-Reducing-The-Cost-Of-Anti-Money-Laundering-Compliance.pdf
18. https://home.kpmg.com/xx/en/home/insights/2014/01/global-anti-money-laundering-survey.html
19. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf *(ibid)*
20. http://www.bis.org/press/p140115.htm
21. http://www.wolfsberg-principles.com/
22. At an estimated cost to British business of £1.1bn - £2bn https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/357543/itc-regs-2013.pdf

Figure 1
Q: How concerned are you about the impact of tax evasion on your business in the next 1-2 years? (n=198)



Regulations meanwhile have become more difficult to administer. Russian sanctions, for example, no longer simply prohibit providing services to named entities, but specifically block financing of particular activities, such as debt or equity issuance or even issuance after a particular date.[23]

The most common complaint, however, is that the whole system is fundamentally inefficient. This is best exemplified in the Suspicious Activity Reports (SARs) regime. In the 2014 reporting year organisations submitted 354,186 SARs[24], 82 per cent of them from banks. Most were classified "for intelligence value only"; 14,155 were requests for consent from the NCA to approve high-risk transactions. Only about 1,000 were refused – little more than a quarter of a per cent of the total number SARs.

Again, it is not just those in banks that are critical of this system. "[W]e know the SARs regime is not fit for purpose... It is simply a defensive process adopted by banks to meet regulatory or legal requirements," says a senior figure in the police.

The NRA found criticism was widespread: "Supervisors and private sector representatives consulted in the course of producing the NRA voiced repeated criticism of the SARs regime."[25]

In this respect, costs are just a symptom of a culture of "compliance for compliance's sake," as one bank professional puts it. The system is no longer focused on providing information to help catch criminals, agrees another.

23. https://www.gov.uk/government/news/doing-business-in-russia-and-ukraine-sanctions-latest
24. http://www.nationalcrimeagency.gov.uk/publications/464-2014-sars-annual-report/file
25. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf *(ibid)*

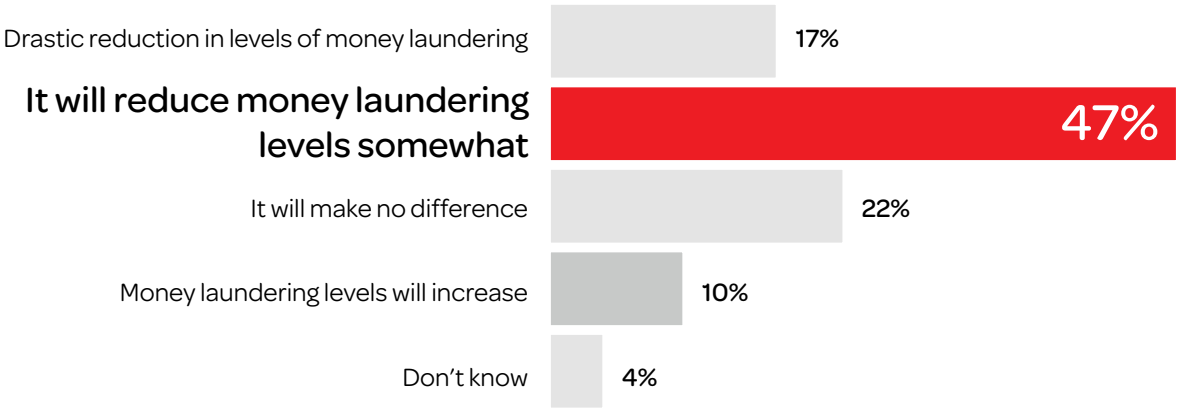
"It's morphed over time into just a process by which we avoid being busted by the regulators," he says.

The prospects for change are mixed. On the one hand, there is the encouragement of the government review into the efficacy and efficiency of AML and CFT announced in August[26] this year. On the other hand, there is continuing regulatory change, with the Fourth EU AML Directive. Intended to put greater emphasis on a risk-based approach, it nevertheless increases requirements, particularly around politically exposed persons and beneficial ownership – not always with good cause.

"The fact that we are legally obliged to treat domestic PEPs as high risk, regardless of any other risk factors, is, to be blunt, regulation for regulation's sake," says one bank's head of financial crime. "It is not effective risk management; it does not factor in the risk profile of either the country or of the PEPs themselves."

Almost a third (32 per cent) of respondents to our survey say that the Fourth EU AML Directive will have no effect or even increase levels of money laundering across Europe, while 47 per cent predict it will decrease it "somewhat". Fewer than one in five (17 per cent) expect the Directive to have a dramatic effect (See Figure 2).

Figure 2
Q: When implemented, what impact do you think the Fourth EU AML Directive will have on levels of money laundering across Europe? (n=198)



26. https://www.gov.uk/government/news/financial-red-tape-targeted-in-new-review

More generally, banks say what's needed is not yet more regulation, but better enforcement. More than 60 per cent say there is enough (31 per cent) or too much regulation (30 per cent), but not enough or "weak" enforcement. Only 6 per cent say that enforcement as well as regulation is too severe.

Ultimately, something has to give. The current system with its ever-increasing costs, wasted effort, and ineffective results is unsustainable in the long-term – at least without significant change within the banking system.

"I don't think that we can continue as we currently are," says one money laundering reporting officer (MLRO). "You just think there is a tipping point and you can only do so much."

1.2 Considering the consequences

Without improvement, a number of consequences look likely.

Most obviously, there is little chance that the effectiveness of the current controls in detecting and deterring crime will improve. Significantly, however, it also has the potential to make things worse.

First, there will be greater potential for failures in processes and systems as they creak under the pressure of an expanding workload. Regulatory complexity adds to this risk. To take a sanctions example, restrictions on "dual use" goods with military and domestic purposes provide an added complication for compliance teams. Banking staff are being called on to evaluate not just the customer, but the nature of the goods and the potential use of sometimes multifaceted equipment – a task for which staff have no qualifications.

One consequence of this is that increasingly financial crime goes undetected. Another is the de-risking we already see. Unable to ensure compliance – or at least to do so affordably – in respect of certain types of client, banks have withdrawn from certain markets, sectors and geographies. Money service bureaus[27] and charities[28] have been among those badly hit; so too have correspondent banks, particularly in emerging markets.[29] Despite efforts of the inter-governmental Financial Action Task Force[30] and the FCA[31] there is little sign that the practice will cease while the current regulatory environment endures.

A number of risks result from de-risking. For the banks themselves, there is the potential of an additional regulatory enforcement risk if the FCA grows frustrated with banks' failure to address its concerns over de-risking. As part of its AML work, the FCA has said it will now look at whether firms' de-risking strategies give rise to consumer protection or competition issues[32] – a "thinly-veiled threat", says one legal commentator.[33]

27. https://www.fincen.gov/news_room/nr/html/20141110.html
28. https://www.fca.org.uk/about/what/enforcing/money-laundering/derisking
29. http://www.globalbanking.org/reports/De-Risking-CBR-Summary-Report-Formatted-v4.pdf
30. http://www.fatf-gafi.org/documents/news/derisking-goes-beyond-amlcft.html
31. https://www.fca.org.uk/news/support-financial-action-taskforce-work-de-risking-drivers
32. http://www.fca.org.uk/about/what/enforcing/money-laundering/derisking
33. http://www.out-law.com/en/articles/2015/april/fca-effective-anti-money-laundering-strategies-should-not-include-wholesale-derisking/

Another risk is displacement. Legitimate customers and criminals affected by de-risking – and even those that are not, but just tired of delays resulting from compliance – will move to other, less tightly regulated channels to move money, whether smaller banks (where the FCA has noted that controls are weaker[34]), alternative providers or alternative jurisdictions. Banks already report seeing this, with customers setting up subsidiaries in less regulated jurisdictions to handle difficult transactions, for example. As a result, AML and sanctions regulations are effectively reducing the visibility and control over the financial system.

"You move the financial crime risk... [and] then the fraud goes unnoticed, unrecorded, un-dealt with. It's a big issue," says a senior policeman.

Alternative channels are also likely to grow – and are likely to be more attractive since AML requirements have hit customer service levels in banking.

"[T]he customer is being completely forgotten in all of this," says one banker. "We've now got customers having quite horrendous on-boarding experiences and having assets frozen inappropriately just because maybe a team's made some incorrect assumptions."

This reduced level of service may yet also come with a higher price tag. If the costs of compliance continue to run into the billions for large banks collectively, it is not hard to see this calling into question the future of free banking – a long-term feature of the UK retail market.

Alternative providers, meanwhile, may come from not just those looking to capitalise on the established banking sector's difficulties; we may also see states looking to limit their vulnerability to sanctions – as evidenced by Russia's enthusiasm to develop an alternative to the SWIFT payments system.[35]

Finally, the combination of the strain on banks, moves to de-risk, and increasingly ambitious sanctions regimes creates a potential systemic risk. "What if similar sanctions to those imposed on Russia are applied more widely, perhaps across the Middle East and Africa to combat Islamic State," asks one bank professional.

"When they apply it to other countries and it's happening across the board, it is going to damage the whole international payment network. It will grind certain things to a halt."

Such risks, of course, may never materialise. The future is uncertain. However, this is exactly the point, and perhaps the ultimate failure of the current AML system: it is almost entirely reactive. Fulfilling the tick-box regulatory requirements of AML controls takes precedence over proactive investigations, and little or no time and resources are left for strategic planning.

The real risk, then, is that no one is able to identify the key emerging financial crime threats, because those with the expertise to do so are too busy trying to stay compliant.

34. http://www.fca.org.uk/your-fca/documents/thematic-reviews/tr14-16

35. http://www.forbes.com/sites/kenrapoza/2015/06/01/russia-wants-to-convince-bric-partners-to-create-alternative-banking-system/

2. Getting personal: liability and recruitment

An additional challenge with the growing regulatory burden is its potential to result in compliance professionals disengaging with and even leaving the profession. There is already palpable frustration in the industry with the regulatory load and its perceived failure to actually address the risk of financial crime.

"We're supposed to be anti-money laundering. We are not anti-money laundering; we are [trying to] save ourselves from the regulator," says one senior bank official.

This is particularly dangerous given other pressures, that are increasing demand for compliance staff while threatening the future supply of competent professionals.

The increased demand is largely driven by the regulatory pressure, direct and indirect. The FCA has actively encouraged banks to bulk up their compliance functions. For example, its review of smaller banks' AML and sanctions controls concluded that a third had inadequate resources.[36] The more significant impact on the compliance labour market, however, has come from big banks' response to compliance failings.

HSBC alone hired more than 2,200 compliance staff globally in just the first half of 2015 – principally in financial crime compliance.[37] In August of the same year, Standard Chartered announced a fivefold increase in its financial-crime headcount over the past three years.[38]

In the UK specifically, 2,157 new AML roles were created in the 12 months to August 2014[39], according to one recruitment consultant. According to another, competition and demand for talent are now at their highest level since immediately after the financial crash, with AML, KYC and – more recently – sanctions compliance being key areas of interest and demand.[40]

Big recruitment drives such as those mentioned above are obviously sporadic. However, they are large enough to have a significant short-term impact on the supply of skilled labour, and frequent enough to be almost continual in their effect. There seems little reason to expect this to change, given the intensity of government and regulatory interest in combating financial crime.

Demand for financial crime specialists is being driven by new entrants to the banking industry and other sectors as well. The UK already has seen an increased emphasis on controls within law firms and estate agencies, following concerns of money laundering linked to the London property market.[41] This increased scrutiny, in addition to the new measures required by the Fourth EU AML Directive, will lead to banks becoming more demanding of the standard of compliance in these sectors. This will likely result in new employment opportunities opening up for compliance professionals in industries associated with the property market.

36. https://www.fca.org.uk/static/fca/documents/thematic-reviews/tr14-16.pdf
37. www.hsbc.com/~/media/hsbc-com/investorrelationsassets/hsbc-results/2015/2q-results/hsbc-holdings-plc/hsbc-holdings-plc-interim-results-2015-media-release.pdf
38. http://files.shareholder.com/downloads/STANCHAR/879216637x0x843626/9409318B-6871-46D1-ABA7-3498FFF072BB/SC_PLC_HY_2015_Press_Release_05_August_FINAL.pdf
39. http://www.brightpool.co.uk/additional-information/jump-in-demand-for-anti-money-laundering-expertise-as-banks-face-increased-scrutiny-from-fca/
40. http://www.mlros.com/resources/publications/2015_bs_compliance_2015_uk.pdf
41. http://www.ft.com/cms/s/0/a421beac-3ce7-11e5-8613-07d16aad2152.html#axzz3oqQSrvHQ

In the US, meanwhile, May 2015 saw the first enforcement action against a virtual currency payments platform.[42] As this report discusses elsewhere, this is likely to be a key area of financial crime growth in the future.

These other sectors and new players will not always compete directly with banks for talent, but can nevertheless have an impact in two respects: First, in respect of the supply of contractors, consultancy and temporary staff available to the sector to plug gaps in in-house resources; second, in driving the need for experts within banks who understand the risks of these other participants, since they will be supplying banking services to them.

2.1 A less attractive option

The increase in demand for AML and other compliance professionals is all the more challenging since it threatens to be matched with tightening supply. A number of factors in addition to workloads look likely to contribute to this.

One is the increasing variety of skills required as the risks within the remit of financial crime teams multiply. Those with AML experience and a grounding in emerging risks around cyber crime (and virtual currencies), are in short supply. Regulatory expectations also call for greater depth, as well as breadth, in a compliance team's experience. Consequently, AML professionals are now generally expected to have a professional certificated qualification from bodies such as the Association of Certified Anti-Money Laundering Specialists (ACAMS) amongst others.

The compliance industry is also increasingly specialised, which can reduce its attractiveness as a career option. Candidates may find options within the business and even the compliance sector more limited than in the past. Partly due to the risk that front office staff will use experience in compliance to circumvent controls, opportunities to move from compliance to the front office – a common ambition historically – are now rare.[43]

A far more important influence on the attractiveness of the career are the increasing liabilities professionals find themselves exposed to, however. The increasing range of responsibilities facing AML professionals is matched by an increasing tendency on the part of regulators to hold individuals personally liable – through civil and criminal action – for compliance failures.

US regulators have been most active in this respect. Take for example, the Financial Industry Regulatory Authority (FINRA) fining Brown Brothers Harriman's former global anti-money laundering compliance officer $25,000 and suspending him for one month in 2014. However, the FCA has increasingly little hesitation in holding individuals accountable, too. In 2012/13 more individuals than firms faced enforcement action in the UK.[44] Outside banking, 2014 saw the owner of a money services business jailed after action by HM Revenue & Customs (HMRC) – not for substantive money laundering, but for failures to comply with regulatory AML requirements.[45]

"MLROs have a key role to play in ensuring that firms take appropriate action to minimise the financial crime risks they face. Where individuals fail to meet their regulatory responsibilities we will not hesitate to take action," Tracey McDermott, director of enforcement and financial crime and now acting chief executive, has warned.[46]

42. http://www.fincen.gov/news_room/nr/html/20150505.html
43. Barclay Simpson's survey noted that this was a particular issue within investment banking: "Investment banks invariably prefer to recruit from competitors and are less open to candidates from other sectors. The benefit for compliance professionals is that once they are established in a big investment bank, their services will be in demand. The downside is that their skills are often specialist. This can limit their career development options within both the sector and compliance generally." http://www.mlros.com/resources/publications/2015_bs_compliance_2015_uk.pdf *(ibid)*
44. http://www.fca.org.uk/static/documents/annual-report/fsa-enforcement-performance-account-2012-13.pdf
45. http://www.mynewsdesk.com/uk/hm-revenue-customs-hmrc/pressreleases/money-transfer-boss-jailed-1084958
46. http://www.fsa.gov.uk/library/communication/pr/2012/055.shtml

Such actions are likely to become more common, with the FCA publicly committed to pursuing more cases against individuals and "holding members of senior management accountable for their actions"[47]. Furthermore, from March 2016 it will be supported by the new Senior Managers Regime[48] (SMR) designed to make this task easier.

The regime will make named senior individuals in banks explicitly responsible for particular areas of the business and for any failures in compliance within these. It also coincides with the new criminal offence for senior managers in banks whose reckless misconduct causes their firm to fail.

MLROs, despite some objections, will be accountable under the new regime.[49] The number of cases against them will consequently grow and, irrespective of the size of the penalties, regulatory sanctions could be career ending.[50]

2.2 Counting the cost

A number of consequences flowing from these trends will shape the risk of financial crime and prevention in the coming months and years ahead.

The most obvious is the rising cost of compliance as a result of higher salaries. Competition for staff and the need to compensate for more specialised careers and increased responsibilities are inevitably putting upward pressure on salaries.

In 2014, according to a survey by ACAMS, base salaries for AML/CFT and financial crime prevention specialists in Europe grew 7.5 per cent to a median of $85,675, while a quarter were paid more than $121,634.[51] Other surveys put pay increases in the UK up even further – rising an average 20-30 per cent for AML/KYC professionals[52], according to one.

Even after this, there is still considerable room for increases in compliance salaries. They are likely to come under further upward pressure as a result of the SMR, since this burdens compliance professionals with responsibilities shared only with more senior, higher-paid managers.

"As a branch of an EEA [European Economic Area] passported institution, the two roles that are caught by the Senior Managers Regime are the branch manager and me. I can assure you I do not get paid at the same level as the branch manager," comments one head of financial crime at a large bank. The pay should be commensurate with the risk, he insists.

Such increases in salaries can only add to the pressure to de-risk as the costs of compliance make more business become unviable, with all the consequences outlined earlier.

47. http://www.fca.org.uk/firms/being-regulated/enforcement
48. https://www.fca.org.uk/news/fca-publishes-final-rules-to-make-those-in-the-banking-sector-more-accountable
49. https://www.fca.org.uk/static/documents/consultation-papers/cp15-09.pdf
50. As regulators in the US have acknowledged: "[Action against individuals] has a lot of implications for careers," according to FINRA senior enforcement director Sarah Green. http://www.reuters.com/article/2014/01/30/us-usa-bankers-accountability-idUSBREA0T1UC20140130
51. http://www.acams.org/2015-acams-aml-compensation-survey/
52. http://www.morganmckinley.co.uk/sites/morganmckinley.co.uk/files/UK_Salary_Guide_2014.pdf

Closely related to this is the risk-aversion that liability breeds; the risk of tick-box compliance at the institutional level is present at the personal level as well. Under the threat of personal liability the focus of compliance managers is at risk of shifting from mitigating the risk of financial crime, or even the organisation's risk of compliance failures, to mitigating their own risk.

Indeed, there is increasing scope for the interests of the organisations and their compliance staff to be pitted against each other. In a result of a failure, both may try to blame the other. In criminal cases, the use of Deferred Prosecution Agreements[53] may further encourage this tendency by incentivising companies to incriminate individuals to avoid action against the organisation.

2.3 Mind the gap

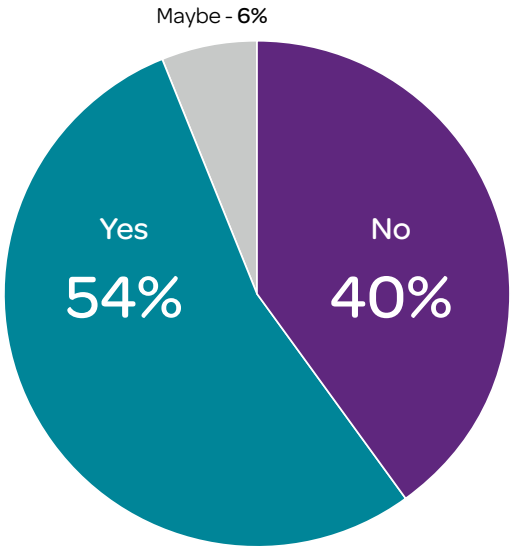
One further and possibly more immediate danger is also worth examining: recruitment difficulties and skills gaps. The scope for this gap can already be seen in the recruitment surges from large banks causing difficulties for others in the industry.

"[W]e're not able to pay what the market would currently be looking at to pay," says one small bank's financial crime head.

The SMR and growth in personal liabilities are likely to exacerbate the gap, as the attractiveness of in-house roles within banks declines relative to lucrative consultancy positions.

This is supported by our survey findings. Shockingly, more than half (54 per cent) of those polled said that in light of increased personal liabilities, they would choose a career path other than financial crime compliance, given the opportunity. Half said the SMR would make their jobs more (40 per cent) or a lot more (10 per cent) stressful (See Figure 3).

Figure 3
Q: If you had the opportunity, would you choose a career path other than financial crime compliance, in light of the increased personal liability? (n=198)



53. http://www.sfo.gov.uk/press-room/latest-press-releases/press-releases-2014/deferred-prosecution-agreements-new-guidance-for-prosecutors.aspx

There is, therefore, a danger of an exodus of experienced staff from banks. As another director of compliance notes: "There are a lot of jobs out there for people with the same skill sets that don't have that liability attached to them."

Asked to predict the biggest emerging financial crime risk to their business in the next 12 months, 13 per cent in our survey cited a lack of personnel in their risk function – the second most popular answer.

Widespread skills shortages will result in positions being filled with less experienced staff, including graduates[54], and inevitably undermine the effectiveness of banks' controls. Improvements in technology and leveraging developments such as big data, meanwhile, can only offset shortages by so much; banks still need expertise to correctly interpret and respond to the outputs from systems and software.

Crucially, however, it is not just banks that suffer from skills shortages. If anything, regulators and enforcement agencies face the more pressing threat from the increase in competition for expertise. As one interviewee at a big bank notes: "We can attract – and have attracted – the best of the NCA, for example, because we say, 'We'll double your pay and give you healthcare.' Why wouldn't you come?"

This situation, again, presents obvious challenges to ensuring effective responses to financial crime. It also does banks no good in the long-term. If state agencies lose their experienced staff, it undermines the chances of developing the intelligently targeted regulation and enforcement that both sides require.

54. [A]cross financial crime and regulatory policy there will be a widespread skills shortage, and as a result employers will potentially hire an increasing number of graduate-level candidates to make up for the shortfall." http://www.robertwalters.co.uk/wwwmedialibrary/WWW2/global/content/salary-survey/2014-global-salary-survey.pdf

3. A joint effort: collaboration challenges

Many of the challenges around skills shortages, as well as the burden of regulation, have at their source a failure to work together. At the very least, greater coordination and collaboration would substantially alleviate them.

This is true in almost every relationship involved in the fight against financial crime: between banks, between regulators, between regulators and banks, and even within individual banks themselves. At its simplest it plays out in significant duplication of efforts.

Within banks, overlaps can be found between the work of KYC, AML and audit teams. Between banks, international payments may be checked through central controls in the head office, under the systems of the correspondent bank, and perhaps also under a different bank's systems, if another correspondent is being used. At least three teams are likely to undertake substantially identical checks.

More broadly, the need for convergence of AML, fraud, sanctions, and anti-bribery and corruption controls within banks has long been recognised – and is gathering pace.[55]

Enforcement too, is fragmented, with the police, Serious Fraud Office (SFO), NCA and HMRC sharing overlapping powers and responsibilities. The range of bodies dispensing regulatory advice, guidance and best practice, and their potential to add to the regulatory burden, has already been discussed.

Duplication not only adds to the costs of compliance and burden of regulation, but also makes it harder for banks to confidently meet regulatory expectations. This is perhaps clearest across jurisdictions, with banks open to class actions from abroad for providing services to UK account holders, even with the explicit approval of domestic regulators. The class action brought against NatWest for providing services to the charity, Interpal, for which it had approval from the Bank of England[56] is a prime example. This issue is the "single biggest worry" currently for one AML practitioner we spoke to.

"It makes your job almost impossible in terms of being able to give the board assurance that they're okay to do business," she said.

Better information flows would also strengthen the fight against crime. More information from agencies such as "watch lists" from HMRC, similar to government lists for sanctions targets[57], would enable banks to target efforts against tax evasion more effectively; clear identification of priorities in tackling bribery and corruption from enforcement agencies would permit more focused, enhanced reporting from banks on those areas.

Likewise, banks' compliance functions could undoubtedly contribute to making enforcement more effective. First, they have a level of insight into the operation of financial networks that could make financial sanctions more effective. Second, better information flows to law enforcement agencies would effectively help centralise information to identify trends and patterns of behaviour, and ultimately anticipate crimes.

Aggregating data reporting is key to "predictive policing", as a senior policeman puts it.

55. http://bis.lexisnexis.co.uk/blog/posts/anti-money-laundering/one-basket-for-the-rotten-eggs
56. http://www.reuters.com/article/2014/09/22/royal-bank-scot-natwest-hamas-idUSL2N0RN13420140922
57. https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

The need for collaboration, internally as well as externally, is only going to become more pressing with the increasing range of risks within the scope of financial crime, from tax evasion to cyber crime.

As one consultant puts it: "[A]nti-money laundering is shifting from a standalone function under compliance, to an increasingly complex and overarching function cutting across legal, risk, operations and tax."[58]

"What [this] cries out for is the bringing together of money laundering, cyber and fraud into one operational arm," says a police source we interviewed.

3.1 Two steps forward...

There has already been substantial progress towards better collaboration at almost all levels.

Encouragingly, its importance is explicitly recognised by the UK Government, which notes: "Increasing collaboration between law enforcement agencies, supervisors and the private sector is essential to help prevent and detect money laundering and terrorist financing, and protect the UK from their effects."[59] Similarly, the last government's Anti-Corruption Plan[60] established its plans to ensure "joined up and collaborative" action across government, civil society, law enforcement and the private sector.

Banks also report a willingness on the part of government to work with the banking industry to tackle financial crime. Praise from figures such as the Home Secretary[61] adds to the impression of efforts to create a genuine partnership.

There have been concrete steps forward, too. November 2014 saw a "landmark" agreement between the Royal Bank of Scotland and the City of London Police to see the bank provide free training and advice on financial crime – hopefully "the first of many", according to the City Police Commissioner.[62]

Even more significant is the JMLIT initiative, announced at a February event hosted by the Home Secretary, the governor of the Bank of England and the FCA chairman.[63] A collaboration between the NCA, Home Office, British Bankers' Association, financial services experts and 10 of the biggest UK banks, it is designed to improve intelligence sharing between all parties. A central hub allows banks to share information such as suspicious activity on accounts not just with the enforcement agencies, but also with other banks – through the NCA, which will act as a conduit. The hope is it will give banks a more complete picture of activity to identify crime.

58. http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/money-laundering-shoots-to-top-of-bank-boardroom-agenda-as-threat-of-criminal-prosecution-becomes-reality-says-kpmg.aspx
59. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf *(ibid)*
60. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388894/UKantiCorruptionPlan.pdf
61. "I've seen real leadership from the banks. Making the UK's financial sector even more hostile to criminals is clearly as much a priority for them as it is for government and law enforcement agencies," the Home Secretary said this February. https://www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum
62. https://www.cityoflondon.police.uk/news-and-appeals/Pages/Emma-Smith-head-of-security.aspx
63. https://www.gov.uk/government/news/anti-money-laundering-taskforce-unveiled

As one consultant explains it: "The joint effort sends out the message that the banks are no longer operating in silos; suspicious accounts will be flagged up to multiple institutions by the NCA, once a suspicious activity report has been received. This will prevent a suspect from repeating similar behaviour elsewhere without being detected, severely limiting their options."[64]

If successful, it seems likely the year-long pilot will be extended – and expanded to other banks.

Such moves are supported by similar initiatives. April, for example, saw the BBA's Financial Crime Alerts Service go live, providing real-time alerts from 12 government and law enforcement agencies of financial crime risks.[65] Again, it would be surprising if there were not more to come.

Finally, within the industry itself, frustrations with inefficiencies and duplication of compliance efforts have spurred some to seek industry-wide solutions for common tasks. Utility models, such as SWIFT's KYC Registry[66] launched last year, provide technological solutions to centralise and effectively outsource some of the back office work, reducing regulatory costs. Industry use of utilities seems certain to increase, and the range of services provided is already expanding into areas such as sanctions and beneficial ownership.

3.2 ...one step back

Significant barriers remain to further collaboration, however.

One is continuing mistrust between the government, regulators and enforcement agencies on the one hand, and banks on the other. The adverse effects of this are acknowledged by the Home Secretary[67], but banks, nevertheless, continue to be "pilloried" in public by major politicians, noted one professional. Perhaps related to this situation are continuing challenges in developing understanding of banking in parts of the government and law enforcement. Even with the best collaboration it will take time to remedy this deficit.

"Much has been gained from the JMLIT process in terms of law enforcement's understanding of banks' attitudes and vice versa. But, while the understanding has increased, it has also exposed the gulf that was there in the first place. You now have a rudimentary, slightly rickety bridge across that gulf, but it is going to take a while to get a decent one with substantial traffic across it," as a big bank MLRO specialist puts it.

The most significant barrier to greater collaboration, however, is regulatory. While protection under the Crime and Courts Act 2013 makes initiatives such as the JMLIT possible, data protection regulations continue to restrict the ability to share information elsewhere. (It's notable that the information sharing between banks under JMLIT is through the NCA, rather than direct.)

As one legal expert has noted, there remain significant conflicts between AML regulations and data protection rules: "This means that multinational banks can find it difficult to comply with one without violating the other – particularly given that different countries incentivise banks to prioritise different regimes."[68]

64. http://pwc.blogs.com/fsrr/2015/03/taking-on-the-money-launderers.html
65. https://www.bba.org.uk/news/press-releases/banks-team-up-with-government-to-combat-cyber criminals-and-fraudsters/#.VieLsal1j_0
66. http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2014/PR_KYC_registry.xml
67. https://www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum *(ibid)*
68. http://www.americanbanker.com/bankthink/data-privacy-and-aml-rules-on-a-transatlantic-collision-course-1076361-1.html

This discord is only going to become more acute with the introduction of stiffer penalties for data protection failures under the EU General Data Protection Regulation[69], which will introduce fines of up to two per cent of businesses' worldwide revenues. Combined with the Senior Managers Regime (SMR), it also widens the scope for misalignments between banks' interests and those of their AML officers. The latter, under the threat of personal liability may prioritise compliance with AML requirements, even if it means breaking data protection requirements (for which they do not carry responsibility).[70]

The Fourth EU AML Directive, meanwhile, as with all directives, will be open to different interpretations by national governments implementing it, opening new possibilities for jurisdictional divergences.

3.3 Be careful what you wish for

Increased collaboration also brings risks as well as rewards.

The first issue is that it should be acknowledged that the public sector's appetite for collaboration may be driven by austerity as well as a belief in its effectiveness in fighting crime. To an extent, banks simply accept that more responsibilities to effectively police financial crime are being put on them.

"There is no point in pretending this isn't about the state trying to pull the private industry into doing its job. It is. You just have to accept that and get on with it," says one MLRO who works closely with government.

An additional danger, however, is that increased collaboration, in the absence of substantive change elsewhere in the regulatory environment, adds to the regulatory burden, with the associated negative implications, and results in more de-risking.

Increased sharing of information increases the data available, the SARs that must be filed, and the fear of potential liabilities for failing to act on the increased level of information. The chances of de-risking are further enhanced if banks see that others have dropped a business or particular sector. Utilities may further exacerbate this, in as much as they go beyond simply centralising data, to also standardise banks' interpretations of the regulator's expectations.[71]

This situation, in turn, leads to one final danger: the development in certain areas of a single, shared approach to AML and financial crime controls. Standardisation taken to this level threatens to not only increase the impact of any de-risking decisions, but could also result in vulnerabilities in controls becoming industry-wide. Rather than having to contend with a variety of banks' approaches to detection and prevention, criminals could focus on circumventing just one. The difficulties in effectively clamping down on money laundering and other crimes to date suggest this is a real risk, in that criminals have proved nothing if not resourceful.

69. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011

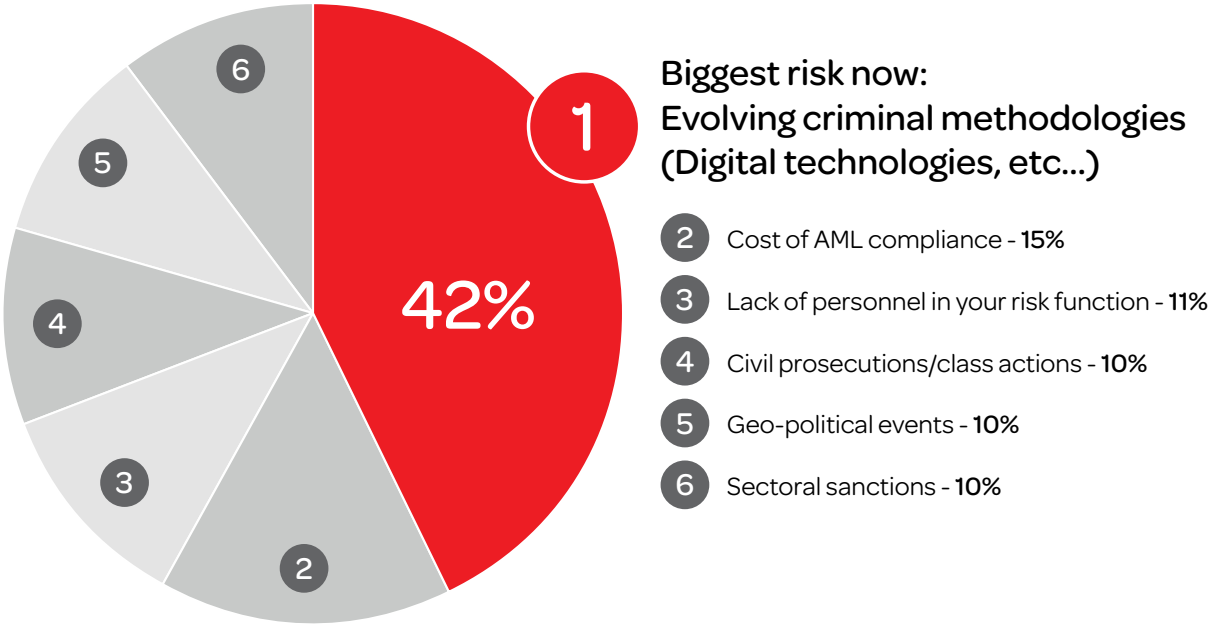
70. http://www.out-law.com/en/articles/2015/september/senior-managers-regime-will-exacerbate-conflict-between-anti-money-laundering-and-data-protection-rules-says-expert/

71. See this article, for example, where the writer suggests utilities may standardise the approach to interpreting sanctions: http://www.efinancialnews.com/story/2015-10-12/industry-should-pull-together-to-combat-financial-crime "Today, for example, individual banks are left to interpret how best to meet regulators' expectations on screening transactions. Fuzzy logic is commonly used to detect possible variations in identity data that suggest similarities to a sanctioned name, but where to draw the line on these variations is unclear."

4. Adapt to survive: technology and changing criminal methodologies

Financial criminals are business people too. When they experience hurdles in the marketplace, they innovate. As a result, financial crime risks are dynamic. Criminal methodologies constantly adapt to discover new opportunities for crime and circumvent the controls designed to prevent it. In our survey, evolving criminal methodologies were considered the biggest single financial crime risk facing respondents' businesses today: 42 per cent naming it, against 15 per cent naming the cost of AML compliance (the next most popular answer) (See Figure 4).

Figure 4
Q: What would you say is the biggest single financial crime risk to your business at the present time? (n=198)



Banks financial crime controls, by contrast, are often reactive – another finding of our survey, which discovered two thirds agreeing that current financial crime risk compliance is focused on reactive prevention.

Identity theft fraud is a good example: Banks are often unable to mitigate new types or methods of fraud until they observe and understand them, by which time they may be pervasive. As a result many bank professionals already feel it is impossible to stay ahead of the fraudsters.

The most obvious examples of criminal innovation in recent times have come from new opportunities for crime from the move to online, mobile and alternative transaction and banking systems. As the NCA has pointed out, this is a particular issue for the UK[72], which the G20 has described as the most cyber dependent economy of its member nations.

72. http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file *(ibid)*

"[T]he move towards an increasingly cashless society will cause a continuing rise in opportunities for cyber enabled fraud and money laundering. The next two years are likely to see a greater range of electronic payment methods become integrated into personal items and commerce," the NCA noted.

For banks, there are of course, significant dangers from now well-established cyber risks, such as hacking and other data breaches. Both large scale attacks[73] and smaller scale breaches[74] at UK banks have emphasised the risk. Investigations of financial institutions by the Information Commissioner's Office, which polices data protection, tripled in the year to April 2015, with big banks the most frequent subjects of investigation.[75]

Banks are "natural targets facing a high threat of cyber risk", according to credit ratings agency Standard & Poor's, adding that it views "weak cyber security as an emerging risk that has a potential to result in negative rating actions."[76]

Even where banks are not directly targeted, they face the risks of fraud resulting from large scale security breaches elsewhere: the attack on telecoms and internet service provider, TalkTalk in October 2015[77] and consequent loss of customer information including bank and credit card details is just one recent example.

The risk is ever-changing. The large scale thefts of the Carbanak gang uncovered in 2015 after stealing up to $1 billion from banks across Russia, the Ukraine, China and elsewhere in Europe, for example, may represent "a new stage in the evolution of cyber criminal activity, where malicious users steal money directly from banks, and avoid targeting end users", according to security firm Kaspersky Lab.[78] Moreover, the NCA has noted that cyber criminals work on new crimeware products at the same time as deploying existing ones.[79]

Given the focus on banks' internal controls and success of spear phishing scams, the next natural progression is perhaps insiders in banks undermining controls.

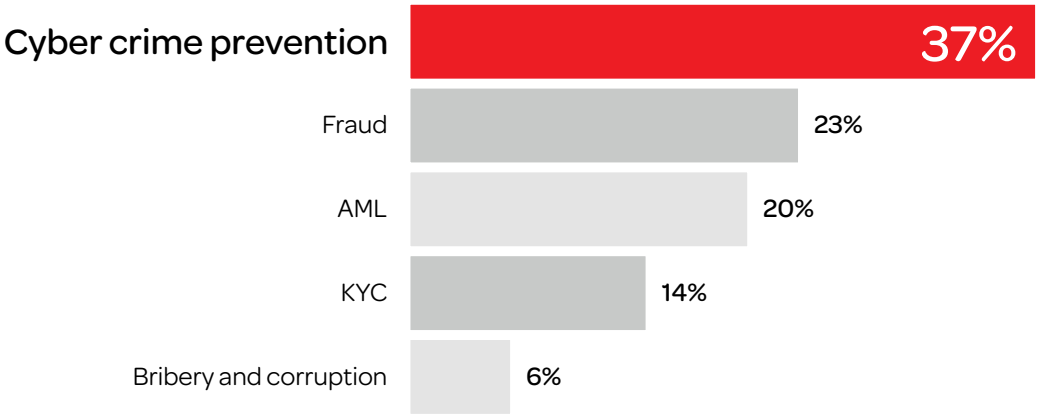
"I would be very surprised if organised criminals were not planting people in banks now," says one bank head of investigations.

In any case, the significance and growth of the risk is likely to make it increasingly difficult for banks' financial crime functions to ignore, adding to the pressure for convergence between cyber risks and more conventional risks. Regulatory pressure, from the FCA's decision to fine RBS for its 2012 IT outage[80] (albeit caused by a glitch rather than a cyber attack), to the addition of cyber attackers to US sanctions lists[81], would seem to push in the same direction.

73. http://www.ft.com/cms/s/0/961a31fa-4a7a-11e4-b8bc-00144feab7de.html#axzz3pNvdclMS
74. http://www.bbc.co.uk/news/uk-england-london-27146037
75. http://www.ft.com/cms/s/0/74314ae6-0943-11e5-b643-00144feabdc0.html#axzz3pNvdclMS
76. https://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1455510&SctArtId=343857&from=CM&nsl_code=LIME&sourceObjectId=9348447&sourceRevId=2&fee_ind=N&exp_date=20250927-20:56:45
77. http://www.bbc.co.uk/news/uk-34611857
78. http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide
79. http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file *(ibid)*
80. https://www.fca.org.uk/news/fca-fines-rbs-natwest-and-ulster-bank-ltd-42m-for-it-failures
81. http://www.reuters.com/article/2015/04/02/us-usa-cyber security-idUSKBN0MS4DZ20150402

Attempts to develop expertise and controls will also add to costs. In our survey, 37 per cent say cyber crime will be the greatest single area of investment in financial crime prevention over the next two years, against 23 per cent for fraud and 20 per cent for AML, the next two most common answers (See Figure 5).

Figure 5
Q: Where do you think the greatest single area of investment in financial crime prevention will happen in your business over the next 1-2 years? (n=198)



Additionally, the BBA highlighted to us concerns over organised criminal groups seeking to defraud banks' corporate and high net worth clients, given the higher returns that the criminals can achieve. Collaboration between BBA members has demonstrated that these groups are operating globally and are laundering their profits into certain jurisdictions where recovery of the stolen funds is difficult.

A range of activities are underway to address these challenges including initiatives with UK and international law enforcement, awareness raising activities and the sharing of expertise among banks on improvements to operational controls.

The BBA also has outlined industry concerns over organised crime use of money mules. Certain categories of bank customers are being targeted by criminals to hold and move the proceeds of crimes on their behalf, both wittingly and unwittingly. By using people that have no adverse history and by laundering high volumes but relatively small amounts of money, detection is very difficult.

4.1 On the move: mobile risks

These risks are enhanced by the growth of mobile banking, particularly in terms of fraud, which shows no signs of abating. Online banking fraud in the UK increased almost 50 per cent from 2013 to 2014.[82]

The use of mobile banking apps doubled in 2013, according to the BBA's figures[83], and in 2015, customers will move £2.9 billion a week using banking apps.[84] In 2020, customers are expected to use their mobile devices to check their current accounts 2.3 billion times – more than internet, branch and telephone banking put together.[85] As mobile phones increasingly take on the role of customers' credit card and bank branch, the opportunities for fraud will continue to grow in scale – and sophistication.

Importantly, an increasing amount of the money moving online is outside the banks' control. Even for their own digital services banks are significantly reliant on third-party providers, introducing a range of potential vulnerabilities.

"Whether it is external data feeds, customer and staff devices or cloud services, banks find themselves having to adapt to relying on systems that are outside their control," notes one board member of the Institute of Risk Management.[86] The proliferation of alternative providers, from PayPal® and Apple Pay® to Bitcoin, meanwhile, has significant consequences for the future of financial crime – as does the adoption of such technology by banks themselves, with JP Morgan Chase, just the latest to announce its mobile payments solution.[87]

One result is a wider range of payment mechanisms available not only to fraudsters but also for use by criminals for legitimate and illegitimate payments. As well as traditional financial channels for transactions such as banks and credit cards, criminals now have a range of options, old and new, including money service bureaus, voucher systems, online payment services and virtual currencies.[88]

The effects will be felt by banks in a number of ways in the future, and pose significant challenges to banks' controls.

The current compliance infrastructure is built around the current banking climate, points out one compliance director.

"[W]hilst that envisages internet banking, it doesn't really envisage people moving [large] amounts of money by mobile technologies or through organisations that don't have the track record of payment processing."

82. http://www.financialfraudaction.org.uk/Annual-Review-2015.asp
83. https://www.bba.org.uk/wp-content/uploads/2014/03/BBA1810_The_way_we_bank_now_2014_PAGES_ONLINE.pdf
84. https://www.bba.org.uk/publication/bba-reports/world-of-change-2/
85. https://www.bba.org.uk/news/press-releases/mobile-phone-apps-become-the-uks-number-one-way-to-bank/#.VioAkql1j_0
86. http://www.ft.com/cms/s/0/4e34c93a-b6d2-11e4-95dc-00144feab7de.html#axzz3pOP1YRoZ
87. http://investor.shareholder.com/jpmorganchase/releasedetail.cfm?ReleaseID=938397
88. https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf

4.2 Losing sight with disintermediation

Long-term, such disintermediation of the banks potentially provides liquidity and even existential challenges. Long before then however, from a financial crime perspective, one impact is a diminishing visibility of customers' transactions and financial affairs, as money increasingly moves through other channels. Even services that link back to the customer's account will only show a payment to the service provider (whether Apple, PayPal or telecoms company). Alternative finance, including peer-to-peer lending and crowd funding, expected to reach £4.4 billion in the UK in 2015[89], compounds this. It is a far cry from the position in decades past where customers held just a current account, a savings account, and perhaps a credit card and a mortgage with their banks.

"[T]he bank has gone from seeing virtually everything that their client did to seeing very little," says one MLRO head.

The risks are not restricted to fraud, as US action against providers such as Ripple Lab[90] around sanctions, CFT and AML have illustrated. The issue will only grow more pressing as the use of alternative channels and the services they provide expand.

Banks also will be forced to evaluate their risk appetite to provide services for these new players, and how they work with them to combat financial crime. On the one hand, most have neither the banks' long experience in tackling financial crime, nor relationships with enforcement agencies. Acquiring that expertise, particularly given skills shortages and rising salaries in compliance, will be costly and take time. On the other hand, some of the new players are huge, such as Chinese giant Alibaba, which launched its own online bank in June.[91]

The banks themselves must therefore also develop their expertise, with most AML practitioners admitting their understanding of many of these new services is low.

4.3 The virtual reality

These challenges are perhaps clearest in the discussions around virtual currencies, which are rapidly emerging as a key risk for the future. Anonymity and the ability to rapidly transfer funds make crypto currencies particularly attractive to criminals, according to Europol.

"Virtual currencies are an ideal instrument for money laundering," it has noted.[92] Bitcoin accounts for 40 per cent of all criminal-to-criminal payments in enforcement investigations.[93]

"Although there is no single common currency used by cyber criminals across the EU, it is apparent that Bitcoin may gradually be taking on that role," the agency states.

For now, virtual currency use, remains mainly the preserve of cyber criminals, but that is likely to change if and when they gain wider acceptance more generally, according to the NCA.

89. http://www.nesta.org.uk/news/alternative-finance-market-set-double-2015
90. http://www.fincen.gov/news_room/nr/html/20150505.html *(ibid)*
91. http://www.ft.com/cms/s/0/e76198d2-1b26-11e5-8201-cbdb03d71480.html#axzz3pbRonQSS
92. https://www.europol.europa.eu/sites/default/files/edi/EuropolReportDigitalCove.html
93. https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf

"[L]aw enforcement can expect to see a corresponding increase in their adoption by traditional (non-cyber) criminals, as a vehicle to launder funds and as a means of payment for illicit goods and services."[94] There also could be considerable scope for crypto currencies to be used to avoid sanctions.[95]

Moreover, even as regulation and transparency of major virtual currencies improves, other currencies and new channels will spring up, and activity will move to where controls are less rigorous. Online games with in-game currencies that can be exchanged for real money are another potential avenue for illicit transfers, for example.

Such risks are poorly understood, admit many compliance professionals, and one obvious response is, again, de-risking.

"[W]e would be very loath to take anybody on now if you know that they are trading in bitcoins because... [w]e don't get it," says one MLRO professional at a bank with only a small retail presence in the UK.

However, de-risking will not prove a sustainable solution as the popularity of such technologies grows. Moreover, to remain competitive, banks must adopt them for their own uses, as the work underway to use Bitcoin's blockchain technology[96] shows. As such, the risks will continue to evolve and grow.

4.4 Taming Blockchain

Blockchain, the technology which underpins Bitcoin, has caught significant attention of bankers across the globe; an interest which was demonstrated at the SIBOS Conference in October 2015, when additional floorspace had to be procured to accommodate a hugely over-subscribed session on the topic.

Indeed, the race to figure out and implement blockchain technology – underway since the early 2000s – looks likely to be the banking industry's version of the space race that preoccupied governments, engineers and technologists in the early 1960s.

Many of the global banks have already started investigating blockchain use cases, and most of these institutions are aggressively investing in and conducting blockchain research and development.

So far, blockchain technology development has resulted in two separate platforms: permissionless and permissioned. The permissionless path, the technology that Bitcoin uses, is the most familiar. It is an open platform that thrives on anonymity and secrecy.

One analyst in a global financial services consultancy we spoke to describes the rise of the permissionless blockchain: "The elusive Bitcoin inventor dreamt up this technology to be 'the domain of anarchists,' anti-government, and an outward and visible symbol of rebellion against central authorities. In his mind, the creation of a fully distributed, transparency–driven currency, therefore, was a solution to an existing problem."

The financial crime potential, especially in terms of money laundering, of Bitcoin, which operates on a permissionless blockchain, are well reported and documented, limiting its attractiveness for banks. Leveraging the permissioned blockchain, the second path, is much more intriguing for banks.

94. http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file *(ibid)*
95. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf
96. http://uk.reuters.com/article/2015/09/15/uk-banks-blockchain-idUKKCN0RF24S20150915

Symbiont, a company focused on creating technology to allow programmed financial contracts on both types of blockchains, is currently piloting its blockchain technology with two US top 10 banks. According to cofounder Robby Dermody, every action and every transfer of ownership is immutably recorded on the blockchain ledger itself, which may easily be verified by each of the counterparties. With proper authority, every transaction can be accessed by regulators. This makes money laundering more difficult for financial criminals. Dermody forecasts that in the future regulators won't have to even visit an institution to flip through records to uncover suspicious activity.

"We are building interfaces to our solutions for our clients so that regulators, to the extent legally mandated, can gain a real-time view of market activity, state of holdings, and so on. The regulators would possess privileged cryptographic keypairs on the Symbiont platform, which are like a digital skeleton key that allows them to see the appropriate level of activities with a given instrument, through its lifecycle from issuance to retirement," he says.

"Moreover, the instruments themselves are written in a special programming language, and actually operate on top of the blockchain. This means that in most cases, instead of having a human being responsible for compliance and back-office activities, the code for the financial instrument itself can take care of the majority of it, further reducing risk."

If a hacker entered the blockchain, meanwhile, they couldn't do anything with the transactions.

"If a hacker gets access to a stock issuance, for instance, it couldn't be used or sent anywhere because to perform operations on that security, the hacker would need one of the appropriately privileged digital keys, which are securely stored elsewhere by the market counterparties themselves," Dermody explains. "And if a criminal was able to get through our network and access a security, it would be worthless to him because he would have to ultimately take it back to a regulated institution, sell it and take the cash proceeds. He would immediately be caught with the blockchain itself serving as a full audit log of his unlawful activities."

Nevertheless, it would be dangerous to assume there are no risks, says the industry analyst we interviewed: "It is not inconceivable that some smart person could come along and figure out how to compromise security within permissioned blockchain technology."

Blockchain technology in the future could give rise to fraud. While the permissioned blockchain is an environment where all participants agree upfront that they are going to participate, which helps solve KYC issues, it could be operated by a centralised entity.

In a permissioned blockchain environment like a global payments network composed of, for example, 20 large market participants, the chance of someone or an entity with access simply doing something illegal is a real risk.

That danger goes to the heart of why Bitcoin was invented in the first place, says the analyst: "There is a real risk associated with centralisation," the analyst told us.

Finally, existing technologies are proven. Blockchain – in the uses envisioned – is not. Banks are at the heart of any marketplace because they facilitate the transfer of capital. Due to that responsibility, banks have to be certain that permissioned blockchain technology will make the market more efficient, scalable, transparent – and stable. The system going down and information being lost, is a clear danger to the stability of the financial system.

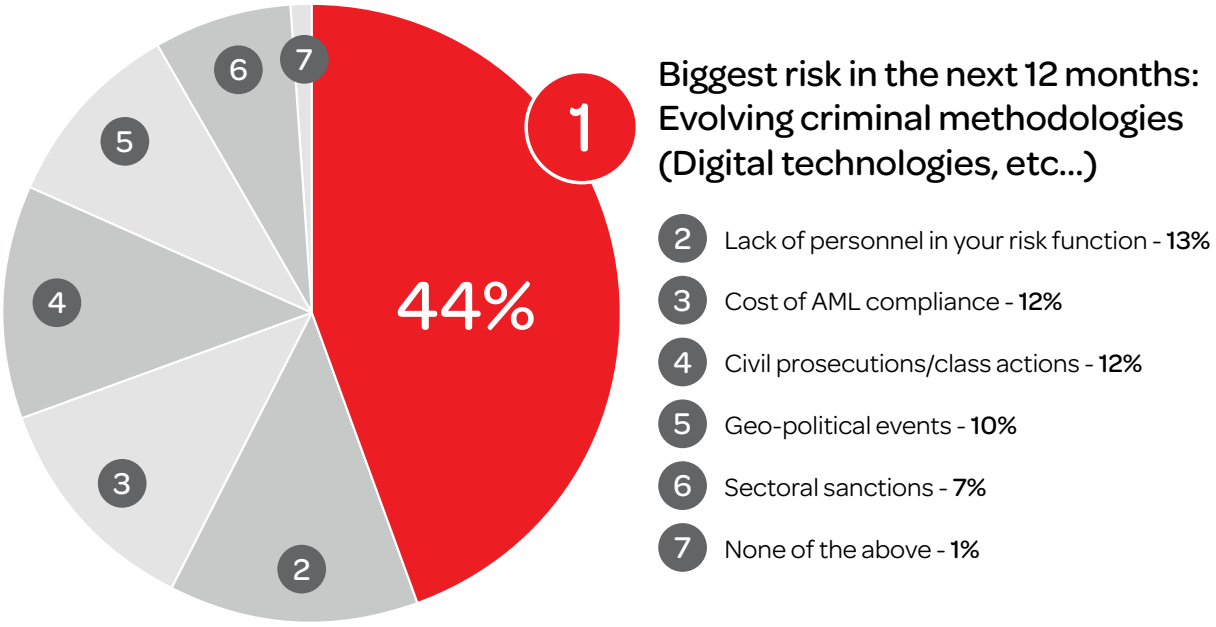
As for whether blockchain creates new kinds of financial crime, as yet unthought of: "Who knows?" says the analyst.

"We'll have to wait and see."

4.5 Unknown unknowns: two steps forward...

Identifying the risks of the future in terms of technology are complicated by criminals' resourcefulness as much as by technological developments. Reactions to banks' controls bring new risks. This can already be seen in activity to attempt to circumvent transaction monitoring systems (See Figure 6).

Figure 6
Q: What do you think will be the biggest single emerging financial crime risk to your business in the next 12 months? (n=198)



"The proper organised criminals, the people who really know what they're doing, have already moved onto transactional monitoring solutions. They already know how they work and configure their attacks [accordingly]," says one director of compliance. This explains why many banks see big increases in fraud attempts over Christmas as criminals look to exploit the difficulty of dealing with the high volumes of activity.

By the same token, new control technologies will in time bring with them new risks as criminals probe for vulnerabilities. The use of biometrics for identification purposes[97] has significant consequences for KYC, for example. In a world where people are no longer known by their Date of Birth and address, but are known by facial features, how does a bank conduct KYC?

Wearable technology, also, will expose new vulnerabilities such as opportunities to steal data, identify and even gain access to payments. Joint Money Laundering Steering Group (JMLSG) guidance on identity verification[98] was written for an age focused on physical documents. However, this focus is likely to become less and less relevant as we move into an ever-increasing digital environment.

97. http://www.rbs.com/news/2015/february/rbs-and-natwest-customers-get-mobile-banking-at-their-fingertips.html
98. http://www.jmlsg.org.uk/

Big data, too, promises to enhance the defence against financial crime and bring its own challenges. The ability to amalgamate and analyse information on countless individual transactions – perhaps all small and legitimate on their own – to identify patterns of behaviour that might indicate suspicious activity has obvious power in the fight against terrorism. However, the scope for false positives just adding to the compliance burden is also significant. Likewise, third party data such as social media has significant scope to improve understanding of customers, allowing banks to build alternative credit scores, for example. Given too much weight or handled incorrectly, however, the same information can be abused by criminals creating false online identities.

Ultimately, the risks of tomorrow will be shaped as much by banks' controls, as changes in technology. Taken to extremes, successful controls will succeed in simply displacing the risk and pushing it offline. It's notable, for instance, that for many criminals cash is still king.[99] In any case, many of the future financial risks online and offline will be shaped by geopolitical changes, whether risks from the activities of ISIS or Russia, or developments in Syria or the Chinese economy. The migration crisis alone could come to place significant pressure on financial institutions conducting appropriate checks to bank newly arrived, often undocumented individuals. Other threats are yet to even begin to emerge.

The one constant is change, which is why banks must continue to look ahead. The fight against financial crime is not one that can ever be fully won, but a failure to adapt to the changing landscape will mean the losses grow more serious each day.

99. https://www.europol.europa.eu/content/cash-still-king-criminals-prefer-cash-money-laundering

Methodology

LexisNexis Risk Solutions used two primary research methodologies to complete this report. Between May 2015 and August 2015, LexisNexis Risk Solutions conducted in-depth interviews with nine senior level financial crime and AML compliance professionals working for banks in the UK and two interviews with senior level law enforcement officers dedicated to fighting financial crimes. The key findings derived from the interviews were tested with the BBA Money Laundering Advisory Panel that comprises senior financial crime professionals from over 30 banks, of different shapes and sizes. A presentation was also made to the BBA Annual Financial Crime and Sanctions Conference alongside a panel discussion.

In addition, during October 2015, LexisNexis Risk Solutions conducted an online survey of senior level AML compliance professionals working for banks and other financial institutions in the UK. The survey generated 198 completed responses.

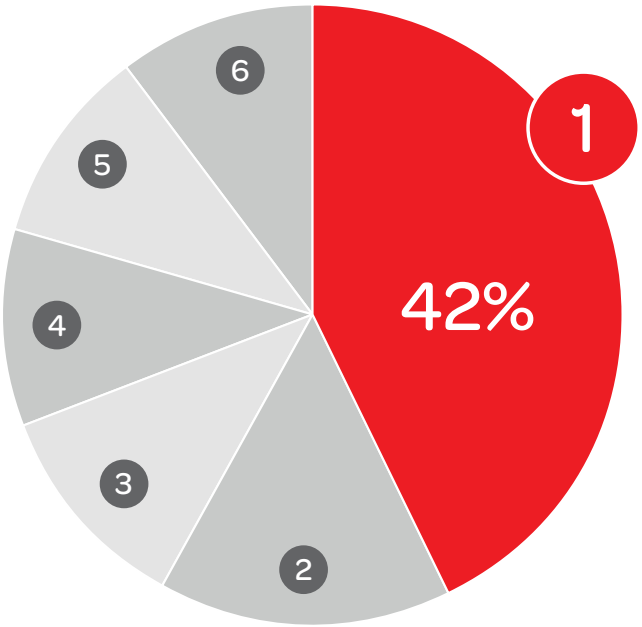
The rich content collected through both methodologies required extensive analysis, the results of which are included as this report.

To continue this conversation and share your insights, experiences and concerns, please contact us at ukenquiry@lexisnexis.com or call **029 2067 8555**.

Appendix

The following diagrams highlight the results of the survey of senior level AML compliance and financial crime professionals working for banks in the UK. The survey generated a total of 198 completed responses.

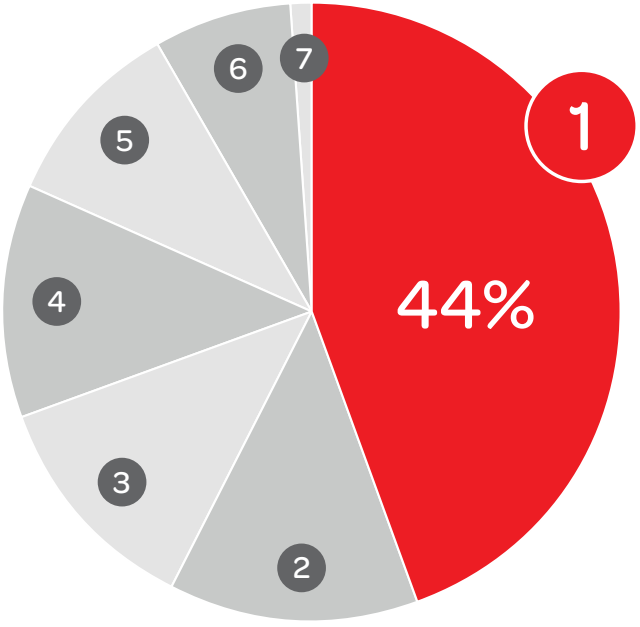
Q: What would you say is the biggest single financial crime risk to your business at the present time? (n=198)



Biggest risk now: Evolving criminal methodologies (Digital technologies, etc...)

2. Cost of AML compliance - **15%**
3. Lack of personnel in your risk function - **11%**
4. Civil prosecutions/class actions - **10%**
5. Geo-political events - **10%**
6. Sectoral sanctions - **10%**

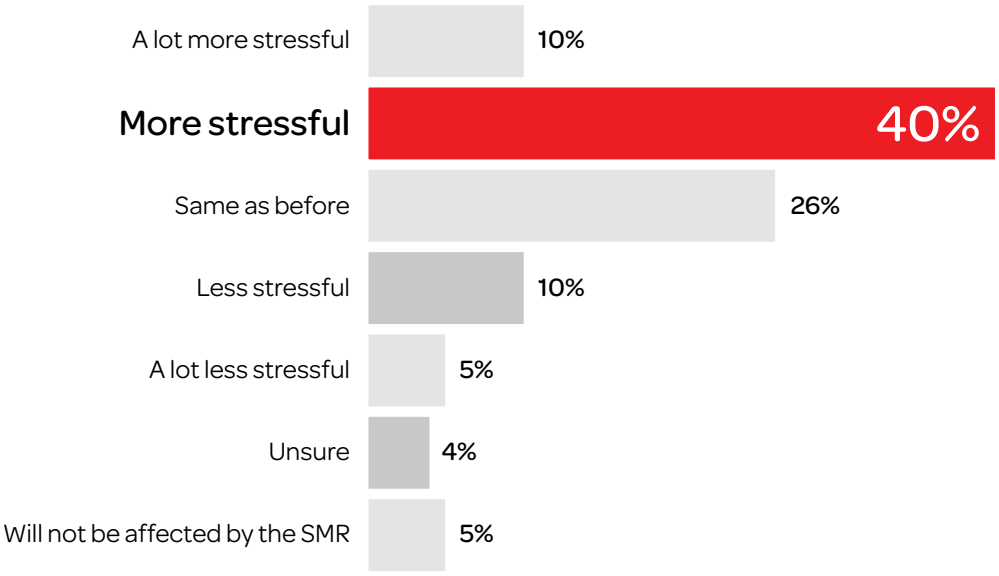
Q: What do you think will be the biggest single emerging financial crime risk to your business in the next 12 months? (n=198)



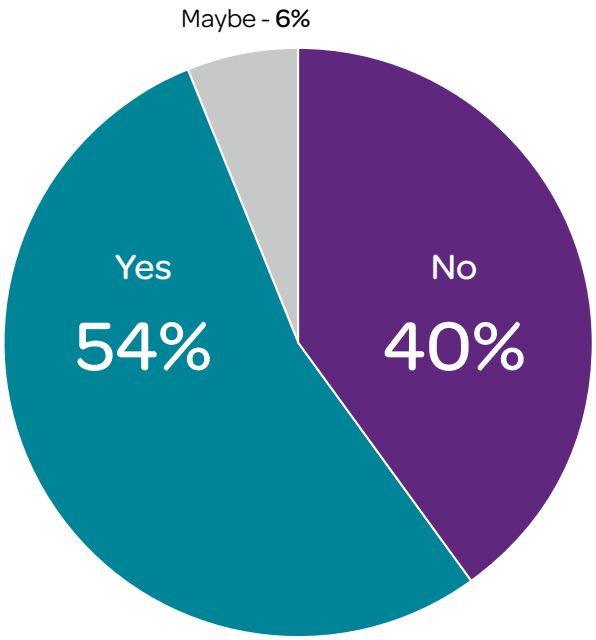
Biggest risk in the next 12 months: Evolving criminal methodologies (Digital technologies, etc...)

2. Lack of personnel in your risk function - **13%**
3. Cost of AML compliance - **12%**
4. Civil prosecutions/class actions - **12%**
5. Geo-political events - **10%**
6. Sectoral sanctions - **7%**
7. None of the above - **1%**

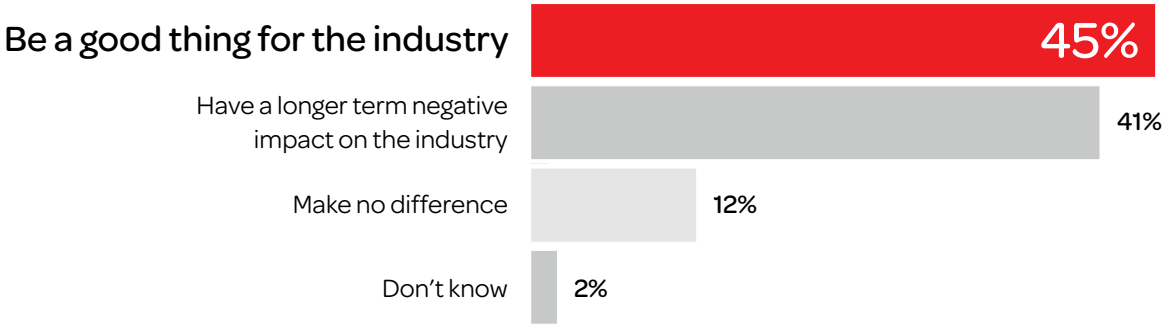
Q: The Senior Managers Regime will bring with it significant additional personal responsibility for MLROs. If you will be in scope of this programme, what effect do you expect it to have on your job? (n=198)



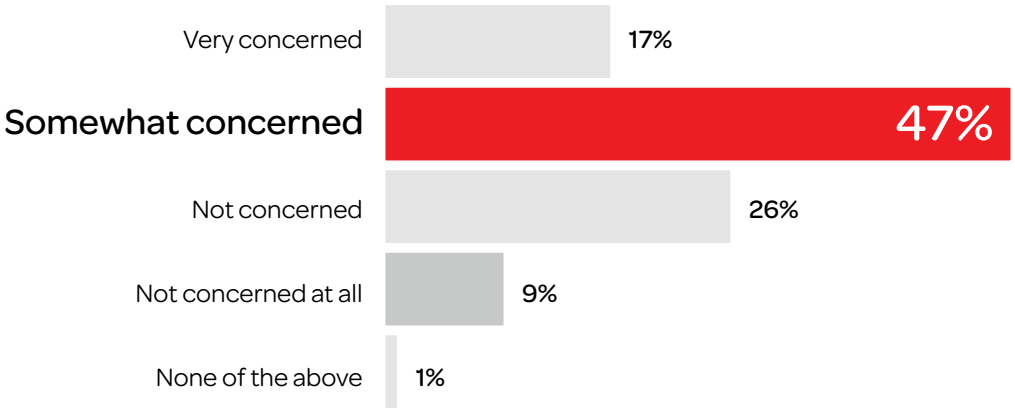
Q: If you had the opportunity, would you choose a career path other than financial crime compliance, in light of the increased personal liability? (n=198)



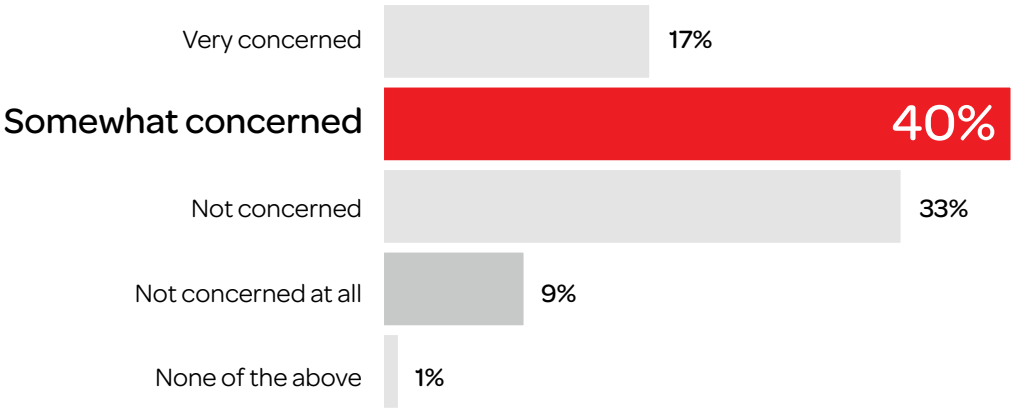
Q: Overall, do you believe making executives criminally responsible for the actions of employees within their firms will: (n=198)



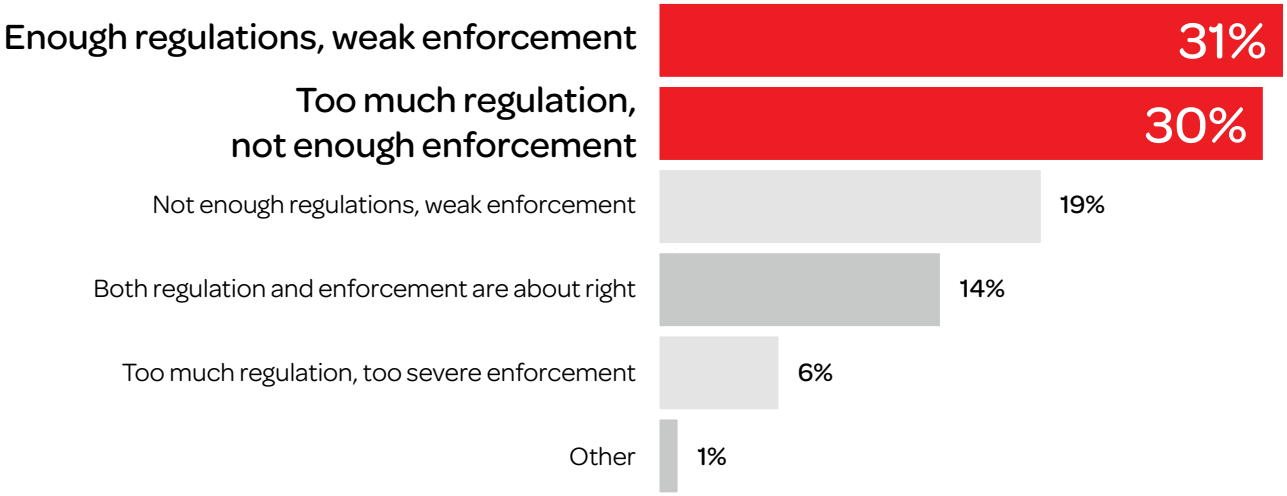
Q: How concerned are you about the impact of tax evasion on your business in the next 1-2 years? (n=198)



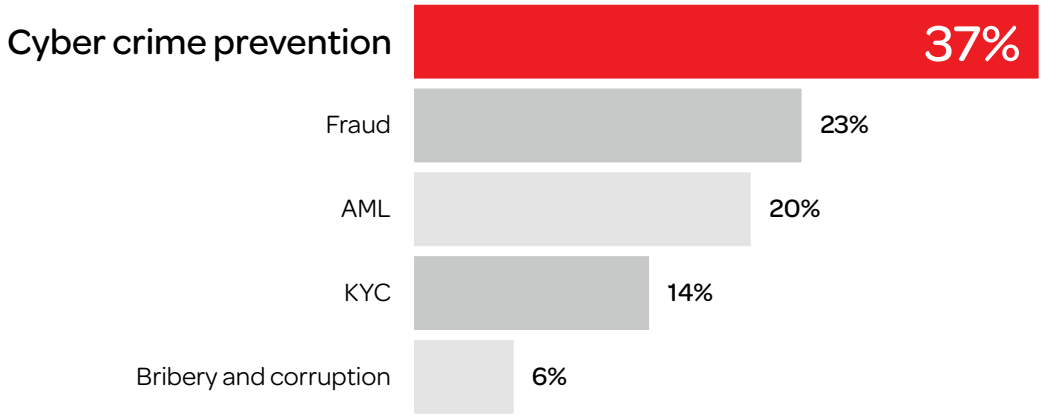
Q: And how concerned are you about the impact of corruption on your business in the next 1-2 years? (n=198)



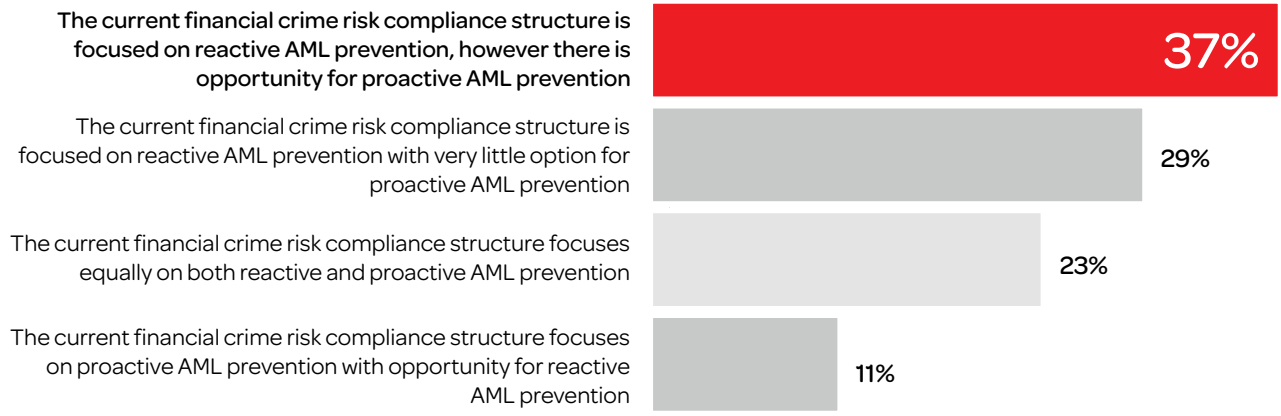
Q: How would you describe the current overall levels of financial crime regulations and enforcement in the UK banking sector? (n=198)



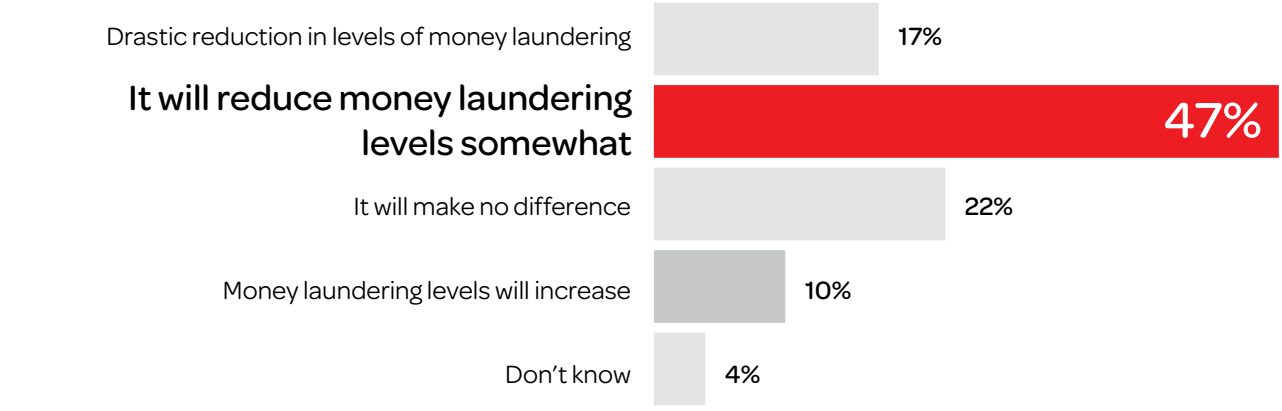
Q: Where do you think the greatest single area of investment in financial crime prevention will happen in your business over the next 1-2 years? (n=198)



Q: Which of the following statements do you most agree with? (n=198)



Q: When implemented, what impact do you think the Fourth EU AML Directive will have on levels of money laundering across Europe? (n=198)



For More Information:

Call 029 2067 8555 or email
uk-irl-enquiry@lexisnexisrisk.com

risk.lexisnexis.co.uk

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, 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. For more information, please visit LexisNexis Risk Solutions and RELX.

LexisNexis® RISK SOLUTIONS

bba The voice of banking