LexisNexis®
RISK SOLUTIONS

Future Financial Crime Risks 2017

A view of the current and future financial crime risks faced by banks in the UK

Table of Contents

Introduction

In 2015, LexisNexis® Risk Solutions produced Future Financial Crime Risks[1], for the British Bankers' Association, a report which identified financial crime compliance issues and potential future risks in the UK. It revealed widespread concerns over growing regulatory burdens, increased personal liability, and barriers to collaboration between banks, regulators and law enforcement. The report also highlighted significant challenges owing to the pace of technological change, innovation and criminal methodologies.

Since then, market conditions have continued to develop at speed, additional regulation has been passed, public-private partnerships have been forged, new legislation has been advanced, geo-political events have changed the status quo and financial crime has continued to evolve. This latest report provides fresh insight and market opinion on the financial crime challenges the UK faces in 2017, how financial organisations are coping with them and how the industry has changed since 2015.

Delivering the insight of senior financial crime leaders at major banks, gleaned during in-depth interviews, and incorporating the broader opinion of senior financial crime practitioners in the UK, collected via an online survey, Future Financial Crime Risks 2017 addresses a wide range of issues impacting financial crime compliance – both today and in the future:

- What is the reaction to the AML Action Plan and Criminal Finances Act 2017? Will these address previous barriers to collaboration?
- Will the benefits created by the Joint Money Laundering Intelligence Taskforce (JMLIT) continue through the Criminal Finances Act 2017?
- What impact has the Senior Managers Regime had and what are UK banks doing about it as a result?
- Are the drivers for "de-risking" still the same?
- How is the financial industry responding to forthcoming legislative developments?
- What are the root causes and unintended consequences of increasing compliance costs?
- How does the utilisation of technology and pace of change compare to criminal methods? What are the options being considered by banks?
- How are Brexit and other geo-political events impacting UK banks?
- What is the biggest single financial crime risk banks in the UK face at the present time? Will it be the same during the next 12 months?

1. https://www.tracesmart.co.uk/insights/future-financial-crime-risks-download

Key Findings

Current sentiments about the state of financial crime compliance remain mixed among UK banks. Whilst there is uncertainty and regulatory fatigue, organisations also recognise improvements and opportunities.

The financial crime professionals interviewed mentioned terms such as “unclear”, “overwhelmed”, “inconsistent”, “confused”, and “complex” when asked their opinion on the financial crime compliance landscape during 2016. These expressions relate to:

- **Feeling overwhelmed / pressured** by the additional regulation they have to understand and act on;
- **Greater uncertainty and anxiety driven by regulatory complexity,** which results in more stringent compliance checks, over-reporting and micro-management;
- **Frustration with the impact of legacy technology** as a barrier to keeping pace with financial crime and managing the cost of compliance effectively;
- **The wrong focus** whereby faster criminal methods conflict with an overburden of regulations not focused in areas of effectiveness, creating “tick box compliance” behaviours rather than (or leaving time and resources for) fighting financial crime;
- **Lack of skilled senior leaders** to deal with the above;
- **Lack of organisational buy-in existed** for some, with front-office functions failing to prioritise middle/back-office compliance needs or intra-company cultural differences and policy hindering the open sharing of information across jurisdictions;
- **Increasing cost of compliance** that continues to put pressure on profitability; and
- **Uncertainty about the direction of future sanctions and regulations** due to recent political change such as Brexit and the Trump administration.

Yet, feedback and survey findings also identify many bright spots, including:

- **A new culture of greater trust** between banks, regulators and law enforcement which has enabled greater collaboration and information sharing; JMLIT has been deemed a success and the Criminal Finances Act 2017 is tentatively seen as a positive step for the legal underpinning of continued information sharing in the UK;
- **Optimism** that increased information sharing between banks and law enforcement can lead to more actionable and informed Suspicious Activity Reports (SARs), thereby strengthening the fight against financial crime and enabling best use of resource;

- **Perceived benefits from the Senior Managers Regime (SMR)** such as creating more accountability, greater collaboration between business and compliance units, increased senior management attention to middle / back-office compliance requirements and heightened opportunities for process efficiencies. Those who have experienced these benefits feel more equipped to fight financial crime and are more likely to indicate that their risk appetite has not been negatively impacted by increased accountability.
- **Less impact by the SMR on hiring and retention than anticipated.** Many survey respondents said that SMR hasn't impacted their ability to fill positions or retain current employees.
- **More confidence than concern about the impact of Brexit** on the Financial Crime Compliance community. The prevailing thinking is that the UK will still largely draw on EU derived legislation, at least in the short term. Nearly half of survey respondents said they expect Brexit to make the UK more accountable with a stronger international voice in terms of fighting financial crime.

These mixed perceptions indicate that pressures remain high but that progress is being made to more effectively manage financial crime in the future. Information sharing and technology will be critical in making this happen. These key factors impact much of the compliance process, outcomes, results and overall levels of frustration.

- **Information sharing** affects the quality of decision making, length of risk exposure, anxieties about risk and liability, and ultimately the cost of compliance.
  - » Information blind spots lead to an increase in the number of false positives being escalated, prolonged exposure to risk, the acquisition of unknown risks, an increase in operational inefficiencies, growing frustrations and potentially lost business.
  - » Intra-bank information sharing across geographic jurisdictions also remains a barrier. Different cultures and priorities within the same bank can reduce information sharing and make it harder to meet compliance requirements.
- **Technology** impacts effective access to information, its distribution, and the ability to analyse and utilise it for actionable decisions.
  - » Disparate legacy systems become a barrier to each of these, which leads to more manual work, less informed decisions, reduced information sharing capabilities, potential human errors and ultimately a higher cost of compliance.
  - » Internal technology is currently not keeping pace with crime and could become a barrier to fighting it.

Key industry trends include:

- **More specialised skills hiring and focused recruitment;** the increased complexity of regulations and crime is shifting the focus from mass hiring towards hiring financial crime professionals with specific compliance-related skills, and even looking outside of the traditional skillset for technologists.
- **Banks are taking more of a case-by-case approach to de-risking** influenced by a variety of different factors.
- **Compliance costs continue to rise,** driven by increased regulatory volumes and complexity, which in turn drives more human resource hiring and technology investments along with fear of the cost of failure.
- **RegTech companies could become an alternative** to costly system upgrades and overhauls, though some banks are adopting a "wait and see" attitude.
- **The Trump Administration is creating concern** around the direction and nature of future US sanctions and US banking regulations.

The following chapters of this report provide more detail on these key findings. The purpose of this report is to support the hard work that has been started in bringing various stakeholders together to tackle the financial crime challenges that hold back the UK economy from its full potential. The report offers the unfiltered thinking and concerns of senior UK financial crime professionals as they seek to balance fighting crime against creating an inclusive and transparent environment for customers and businesses.

We are keen to contribute our own views to the debate and at the end of each chapter there is an observations section, which contains the thoughts of LexisNexis® Risk Solutions on the prior topic. These are easily identifiable as separate from the main body of the report, to ensure transparency.

At this point we would like to thank all participants who kindly donated their time, experience and insight to help make this report as rich and informative as possible.

1. Information Sharing

Key Findings

- **A new 'Culture of Trust' is developing:** The UK Financial Services sector considers public-private industry collaboration, in the form of the Joint Money Laundering Intelligence Taskforce (JMLIT), a success. This marks a significant change from the 2015 report, which identified the need for greater trust between government, law enforcement and financial institutions.
- **The Criminal Finances Act 2017 is (tentatively) seen as a positive step:** The legal underpinning of information sharing is essential for the effective prevention of financial crime. The ability of banks to share information and submit collaborative 'Super-SARs' should result in more actionable and informed reports being filed, facilitating better allocation of resource and improved outcomes at the National Crime Agency (NCA).
- **Cross-Jurisdictional crime remains a challenge:** Organisations continue to face barriers to sharing information across jurisdictions, whether that be within their own organisation or with other firms.

1.1 Knowledge is power

"This year has been quite ground breaking..."

Information sharing for financial crime purposes was an area of significant improvement for the UK financial sector in 2016. The Joint Money Laundering Intelligence Task Force (JMLIT) was heralded as providing significant benefits through greater information sharing and initial results would support this; the Criminal Finances Act 2017 is also expected to continue this work and provide additional benefits.

These initiatives are viewed with significance because they address a critical issue for financial institutions. Nearly all respondents said that a previous lack of information sharing had created negative impacts at one time or another on their organisation and its ability to fight financial crime. As one professional put it, *"what you don't know will very much hurt you."* By not having greater visibility of client information, financial organisations can be impacted by prolonged and unknown risks, compliance process inefficiencies and increased customer friction.

Figure 1: Organisational impacts from lack of information sharing
Source: interviews with senior financial crime professionals at UK banks 11th – 18th November 2016

According to some of the participants, risks associated with limited information could be greater among larger, multinational retail banks. In these companies there are more barriers and siloes in the process in which sharing is limited or blocked between jurisdictions, divisions or business units. Criminals seek opportunity and will operate where information sharing is weakest.

> " Information sharing is quite severe. If you're operating in one jurisdiction, you're inherently sharing with yourself. But when you're dealing globally like us, it's quite clear that criminals use the seams and gaps against us. They move between institutions and jurisdictions – they understand it's complicated from an information-sharing point of view and they take full advantage of these situations."

Respondents told us of cases where requests for information from other jurisdictions within their own global bank have been met with reluctance or apathy; requests were either not prioritised or data was restricted based on cultural differences or national data privacy laws.

There is recognition that information sharing provides benefit to the larger eco-system, including law enforcement - enabling them to better focus resource for optimal outcomes. Without having a mechanism that enables and assures trust in sharing amongst banks and law enforcement, investigations can be impeded and criminal networks can go undetected because there isn't a holistic, 'connect-the-dots' approach. *"I know of important investigations in the City and by the Metropolitan Police whose ability to investigate was impacted by the lack of involvement by certain banks"*, one financial crime investigator from a multinational bank commented. In addition, a senior law enforcement official pointed out that this is about more than just banks, regulators and the police; *"I would hope that we can get across from both a law enforcement and a regulatory side the importance of sharing information because it is for the protection of the public, not only for the protection of the banks."*

According to the National Crime Agency's (NCA) review of JMLIT, in which participating organisations and individuals were surveyed, a significant majority rated this initiative as a success.[2] From our own interviews with UK banking professionals, the cited benefits included a greater level of protection (and indeed legal privilege) to share information with law enforcement, the ability for banks and law enforcement to take more holistic and informed actions together, the ability to learn from each other about processes and emerging threats, and the opportunity to reduce the time that risk might be on a bank's books.

> " The biggest benefit from JMLIT is that the banks have developed a trust of law enforcement and the official side that wasn't there before, and that we've developed a common understanding with law enforcement authorities that there is some middle ground where the banks aren't necessarily the bad guys and law enforcement aren't necessarily the bad guys either".

But there is an even more fundamental benefit of JMLIT, one that is truly ground breaking and perhaps opens a new chapter in the fight against financial crime. Through collaboration of top banks, regulators, and law enforcement, various silos and stereotypes have been overcome; it has enabled a new culture of trust that was previously lacking between these stakeholders and has laid the foundation for further partnership and collaboration.

2. http://www.nationalcrimeagency.gov.uk/publications/708-jmlit-executive-summary-of-fti-report/file; online survey with 169 JMLIT participants and interviews with 46 participants representing JMLIT's Operations Group, Strategic Group and Management Board, conducted by FTI Consulting following conclusion of the 12 month JMLIT pilot

This marks a progression from our survey in 2015. At that time, as JMLIT was relatively new, one of the barriers to collaboration was "continuing mistrust between the Government, regulators and enforcement on one hand and banks on the other".[3] The results make it clear that this issue is being overcome. This was echoed by a senior law enforcement official, mentioning that trust has developed quite quickly based on having opportunity to understand one another, *"Definitely in the past year or so trust has been growing – the first few months I think we were slightly apprehensive, you know, how's this going to work? But the more you get to know one another, the more you begin to trust each other".*

Figure 2: JMLIT successes as detailed in the Criminal Finances Bill factsheet

JMLIT success by the numbers

58 arrests of suspected money launderers

450 bank accounts closed with over £5m suspected of being associated with money laundering

£728,000 worth of suspected criminal monies

In addition to such positive sentiment, JMLIT's success can be readily seen in the numbers.[4]

Recognised by the NCA, *"JMLIT has helped with a number of operations across the whole of law enforcement. More people can be arrested, more assets can be restrained, alerts can be put out to banks to warn them of issues, red flagging these sort of things. So yes, I think there are some very practical things that have happened from it".*

Whereas JMLIT was the pilot for greater collaboration and information sharing, its success as a public - private partnership created a model which, through the Criminal Finances Act 2017, can be applied across the industry. Having received Royal Assent on 27th April 2017, the Act has a wider focus than just information sharing; however, any expansion of sharing within the industry is likely to support the Act's other measures.

3. 2015 Future Financial Crime Risks, a LexisNexis Risk Solutions report produced for the BBA, November 2015
4. Criminal Finances Bill Factsheet, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/559958/Action_Plan_for_anti_money-laundering_and_counter-terrorist_finance_-_consultation_on_legislative_proposals__print_.pdf

Specifically and as part of the Action Plan for Anti-Money Laundering and Counter Terrorist Finance, the Act includes measures to:

Figure 3: Criminal Finances Act 2017 measures[5]

Measures in the Criminal Finances Act 2017

- **Enhance the ability to investigate** proceeds of crime through Unexplained Wealth Orders, whereby individuals whose assets are disproportionate to their known income will need to explain their origin
- **Improve the capability to recover** the proceeds of crime
- **Fight terrorist financing** through complementary changes to legislation governing law enforcement response to terrorist financing threats
- **Prevent the facilitation of tax evasion** through new corporate offences of failure to prevent such activity
- **Strengthen the SARs** regime

It is within the SARs regime measures that greater information sharing is addressed. According to the UK Government, it views the public-private partnership as being *"central to tackling money laundering and terrorist financing"* and adds that *"firm-to-firm information sharing"* will be part of this success.

1.2 Criminal Finances Act 2017*

"You can share with more certainty..."

The Criminal Finances Act 2017 will allow firms in the regulated sector to share information between each other to develop a better understanding of money laundering activities and to use that to communicate with the NCA for support and protection.[6] By also allowing banks to submit joint SARs (i.e., in one comprehensive 'super' SAR), it should result in a more holistic picture being created and provide more actionable intelligence for the NCA, allowing for resource to be more effectively deployed.

Reaction to the Criminal Finances Act 2017 (then the Criminal Finances Bill) was largely positive both during our in-person interviews and online surveys with financial crime professionals. There is recognised value from widening the scope of sharing through peer-to-peer communications, with the anticipation that once implemented the Act (and AML Action plan overall) could help deliver better anti-money laundering outcomes.

5. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564464/CF_Bill_-_Factsheet_1_-_The_Bill.pdf
6. Ibid

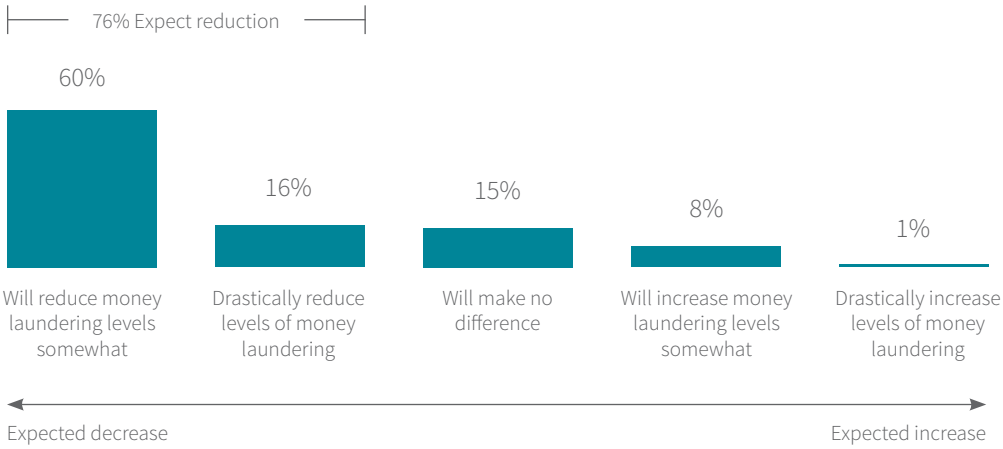
* The interviews and online surveys which generated this report were conducted prior to the Criminal Finances Bill becoming the Criminal Finances Act 2017 on April 27th 2017.

The challenge, as outlined below, will be in implementing the new information sharing powers in an as effective manner as possible in order to help banks deliver the full intended benefits. The intended supporting guidance for this power needs to be as clear as possible to increase information sharing, help improve quality of reporting and support the reduction of unnecessary SARs.

Figure 4

Q: When implemented, what impact do you think the AML Action Plan and Criminal Finances Bill* will have on levels of money laundering in the UK? (n = 168)

Expected impact of AML Action Plan & Criminal Finances Bill* on UK money laundering

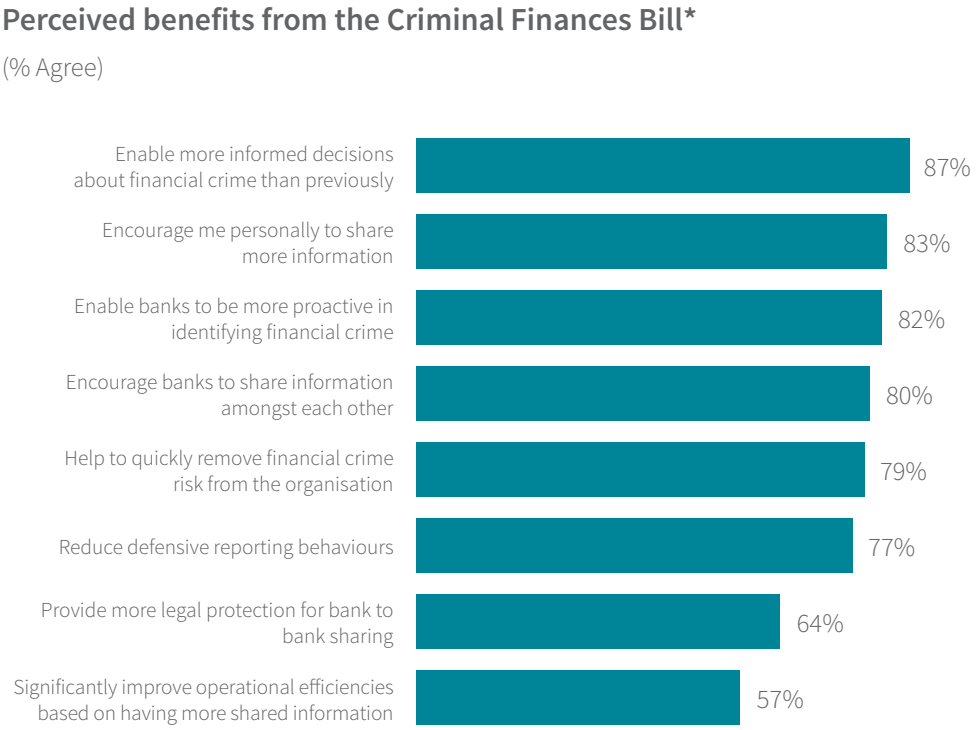


If implemented correctly, the Act is also expected to yield many other benefits to financial organisations, including strengthening decision making, enabling more proactive risk behaviours and enhancing the ability to more quickly dispose of financial crime risk.

* The interviews and online surveys which generated this report were conducted prior to the Criminal Finances Bill becoming the Criminal Finances Act 2017 on April 27th 2017.

Figure 5

Q: When implemented, what impact do you think the AML Action Plan and Criminal Finances Bill* will have on levels of money laundering in the UK? (Respondents could select more than one option; n = 168)



There seemed to be mixed opinion, relating to the improvement of operational efficiencies based on having more shared information. Only 57% agreed with this potential benefit, whilst 36% were uncertain. This is likely due to concerns about where the point of sharing begins; there are those who say that it should be before the legal threshold of reporting suspicion is reached in order to be most proactive and effective (along with other concerns mentioned below).

Law enforcement demonstrated a positive embrace for the Act. One senior crime official mentioned *"where it strengthens the law enforcement response, it's also assisting the public to lose less money and assisting the banks in being able to talk to each other which can only be better because the better intelligence that they've got, the less likely they'll be exposed to losses".*

* The interviews and online surveys which generated this report were conducted prior to the Criminal Finances Bill becoming the Criminal Finances Act 2017 on April 27th 2017.

With this said, the financial crime professionals we spoke with highlighted some concerns:

Pre-versus Post-Suspicion

Some respondents mentioned that the Act needed to allow bank-to-bank sharing at a stage just before the threshold of reporting suspicion, such when there are concerns about transactional anomalies (or even pre-suspicion), rather than waiting for the suspicion threshold to be reached. Otherwise, banks may be less motivated to share what they know. If the institution is already under obligation to submit a SAR, it could feel as though there is no real benefit in sharing further with their peers. Allowing banks to share to confirm or remove suspicion, on the other hand, could enable more proactive and holistic uncovering of financial crime across the industry.

But there could be more to this than just lessening motivation; waiting for suspicion could also prolong the risk. A bank might reach its risk tolerance before suspicion has been generated. As stated by a head of financial crime investigations, *"you wait until you've got suspicion before you share, then the danger is that you've already reached the threshold, so your clock is ticking from the moment you say, we want to share information."*

This sentiment was echoed by a head of financial crime from a leading bank in response to the Call for Information on the Criminal Finances Bill, *"At the stage when information sharing would be most productive in achieving this goal, a bank may not have developed suspicion. However, the provisions of section 339ZB (Disclosure within the regulated sector) only allow relevant undertakings to share information in connection with a suspicion".*[7]

As previously noted, it is essential that this power is implemented as effectively as possible, provided with clear guidance to deliver the full benefits.

Moratorium and Consents

The extension of the moratorium period for investigation into SARs could have negative consequences. Language in the Act allows for an extension period of up to 217 days.[8] Such an extended transaction delay could likely "tip off" the involved party. It could also have an adverse impact on the client's business (even if that client has raised suspicion), prolong potential risk to the bank and cause significant frustration for financial crime professionals.

Data protection conflicts

Our 2015 report mentioned that "the most significant barrier to greater collaboration is regulatory", meaning that data protection regulations could still limit the sharing of information – particularly for multinational banks. With increased sharing of information the challenge of remaining compliant with data protection laws could be heightened and the implementation of the General Data Protection Regulations (GDPR) may further compound this challenge.

7. http://www.publications.parliament.uk/pa/cm201617/cmpublic/CriminalFinances/memo/CFB04.pdf
8. Lexology: Bankers: money-laundering, reporting obligations and the new Criminal Finances Bill, Taylor Wessing; 16 December 2016, http://www.lexology.com/library/detail.aspx?g=538d652d-037b-44de-8979-6a42a33383fb

Observations of LexisNexis® Risk Solutions

Educating consumers on the value of information sharing between organisations

The public perception of information sharing can be varied, particularly in Europe where consumers are less aware of the value it brings to society in fighting challenges such as fraud, money laundering and terrorist financing. Whilst new EU legislation such as GDPR aims to further strengthen and bring some unification to the protection of personal data to the benefit of consumers and society, many individuals are still unaware of how information sharing between institutions can help them directly. When organisations can share information, it builds an inclusive and transparent society – a bedrock for a strong and developed economy.

Cross border sharing of information between Financial Intelligence Units is a good example of how this activity can help fight international money laundering. Eliminating illegal money from the system ultimately means that individuals benefit by receiving the goods and services they request at terms that are acceptable to them, faster and more securely. This could be in the form of online transactions, transfer of investments or application for credit. Conversely, by having access to data that enables them to more accurately assess the risk associated with an individual, the supplier will benefit by being able to identify appropriate terms to offer for services.

Changing this sentiment seems a challenge, but similarly to the benefits derived from the culture of trust that has been nurtured between the private and public sector through JMLIT, developing a relationship of trust between the private sector and consumer could bring significant benefits for the purposes of financial crime prevention.

Education programmes which convey the benefits of information sharing are a step in the right direction to shift the current 'big brother is watching' perception. Financial institutions have the opportunity to lead the way in this respect. By incorporating consumer friendly touch points which highlight the benefits of information sharing into communication campaigns, they can help change public opinion ensuring better service and secure data which can be effectively utilised to create a stronger, safer, more inclusive financial system.

More data can equal more intelligence

The financial crime technology and information ecosystem is highly inefficient. Customer data is often of poor quality and in disparate silos spread across legacy systems further fragmented by business units. This can create significant inefficiencies often leading to the same customer being screened and remediated many times over. In addition, the requirement to screen against wider data sets such as adverse media means that yet more data is being thrown at legacy systems creating significant and often unproductive output, with high volumes of matches having to be remediated. The amount of alerts generated and needing attention can be overwhelming.

This has led to large numbers of people being utilised in an attempt to solve these problems in an inefficient and often ineffective fashion. The end outcome is poor customer experience or worse still commercial decisions being made that result in legitimate custom being turned away.

The ability to obtain a single view of the customer with quality accurate information can help to resolve this problem, and should be considered paramount before any screening or due diligence is conducted. The effective operational sharing of data helps organisations to create a single customer view across the entire business, enabling a true understanding of any given customer and the risks associated with them. This holistic view is vital to effectively combat financial crime and facilitate a more productive customer interaction and experience.

Furthermore, the ability to screen against large amounts of poorly structured data such as adverse media quickly can further strengthen risk assessment and identification. The utilisation of Big Data or other RegTech capabilities can help institutions to achieve this clear view through entity resolution and data disambiguation without the need to undertake significant capital expenditure and making the subsequent processes far more efficient.

Working together for stronger outcomes

The results of JMLIT are truly encouraging and it is a testament to collaboration that this has been achieved. With a permanent legal framework to share information set to be introduced through the Criminal Finances Act 2017, it is essential that the public/private partnership continues to evolve and future strategic opportunities explored.

Legislation is, however, only as good as its implementation, and with sharing only specified at point of suspicion, there is some debate as to whether the measures in the Act will be as beneficial as they could be; the supporting guidance for this power needs to provide clarity to ensure the benefit is fully realised by banks and broader society.

2. Personal Liability and Resources

Key Findings

- **Positive change:** Sentiment indicates the Senior Managers Regime (SMR) has brought about positive change.
- **Positive risk impact:** Three quarters of banks believe the SMR has had a positive impact on their organisation's risk appetite.
- **Little impact on hiring or retention:** Complexity and increased personal exposure doesn't necessarily translate into the career change implied by respondents in the 2015 survey.
- **Increased work challenges:** Whilst the change has been positive, 60% of survey respondents stated it has made their working day more difficult.

2.1 It's not as bad as expected...

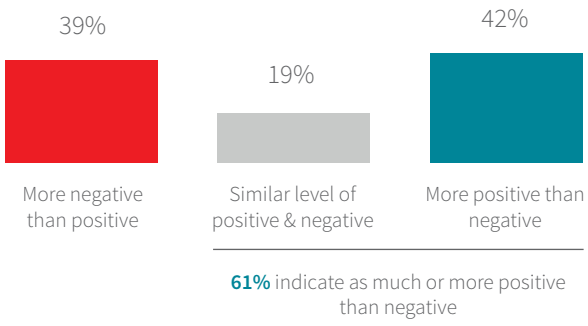
"This has made us focus and make sure that controls are better."

Personal liability and resources have been particularly top-of-mind this past year with the introduction of the Senior Managers Regime (SMR). In our 2015 report the feeling around the topic was one of concern, however, this has seemingly not transpired in reality.

Over half (61%) of survey respondents indicated that its impact has been as much or more of a positive, than a negative, particularly in terms of increasing ownership and collaboration around compliance requirements.

Figure 6:
Index based on number of positive and negative impact statements selected in response to the question detailed in Figure 7 (Which of the following, if any, are ways that the SMR has made an impact on your organisation?) (n = 168).

SMR impact on organisations

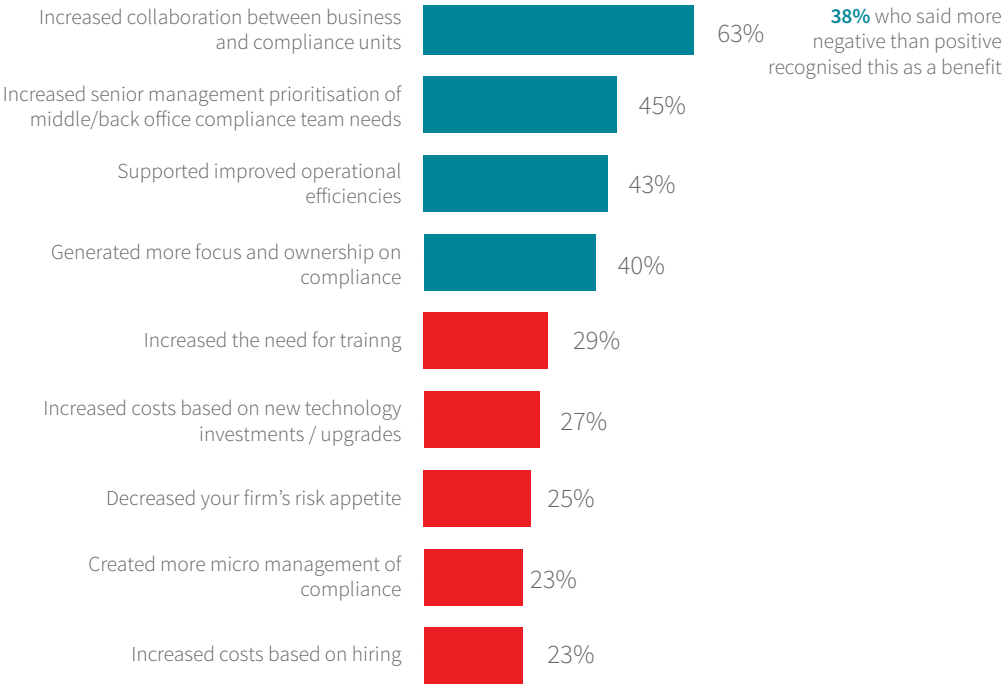


> “ I’ve heard people say in meetings that if things go wrong, they’ll be held liable. And that’s made others sit up and take notice, like that’s a serious role you’ve taken on and I feel obligated to help you with that”

This was evidenced by the types of specific benefits cited, with consensus around those which are positive. Increased collaboration between business and compliance units was the clear winner, even being acknowledged by over one-third of those who indicated a more negative impact from the SMR overall. Additional benefits included increased attention from senior management, improved efficiencies and greater ownership of risk.

Figure 7:
Q. Which of the following, if any, are ways that the SMR has made an impact on your organisation? (Respondents could select more than one option; n = 168)

Top mentioned SMR impacts on organisations



Those who see the SMR negatively were much more fragmented in their rationale, suggesting that their reasons are based on unique organisational issues rather than overall industry trends.

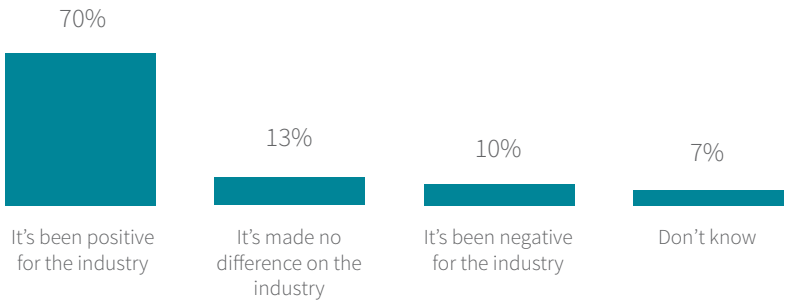
Attestations have made senior executives more sensitive and alert to compliance priorities. Combining these with shifting responsibility to the first line of defence, it has been noted that personal liability has made organisations focus upon greater operational efficiencies in order to remain on the right side of compliance. As mentioned by one senior financial crime professional, *"I think largely because of the FCA emphasis on CEO attestations, there really is a massive shift in terms of first line of defence owning their own risks. They are reshaping the operational methodology to manage this absolutely the right side of compliance".*

In fact, over two-thirds of survey respondents said the policy of making executives personally accountable for employee actions has been positive for the industry itself.

Figure 8

Q. Overall, has the policy of making executives personally responsible for the actions of their employees been positive or negative for the industry? (n = 168)

Making executives personally responsible for employees actions

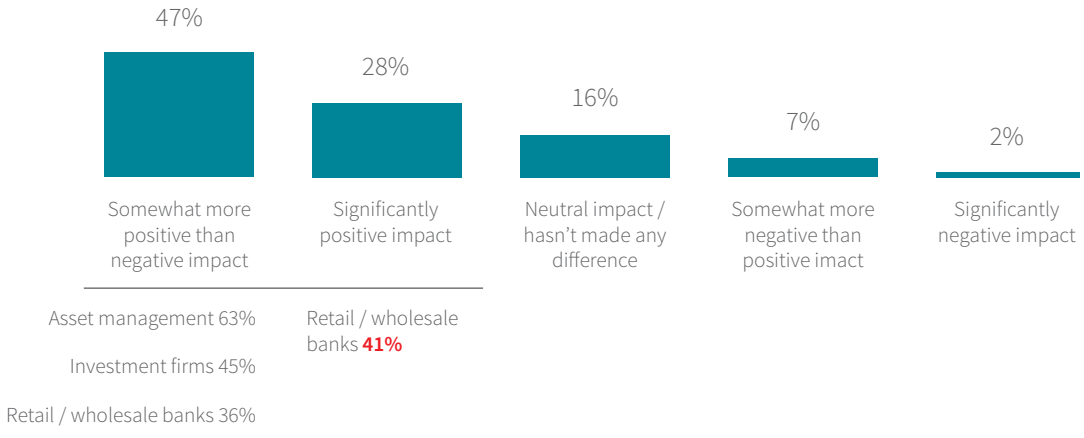


Three-quarters of respondents said that the Senior Managers Regime has had a somewhat (47%) or significantly (28%) positive impact on their organisation's risk appetite.

Figure 9

Q. How would you rate the impact of the Senior Managers Regime (SMR) on your organisation's risk appetite? (n = 168)

Impact of SMR on organisation's risk appetite

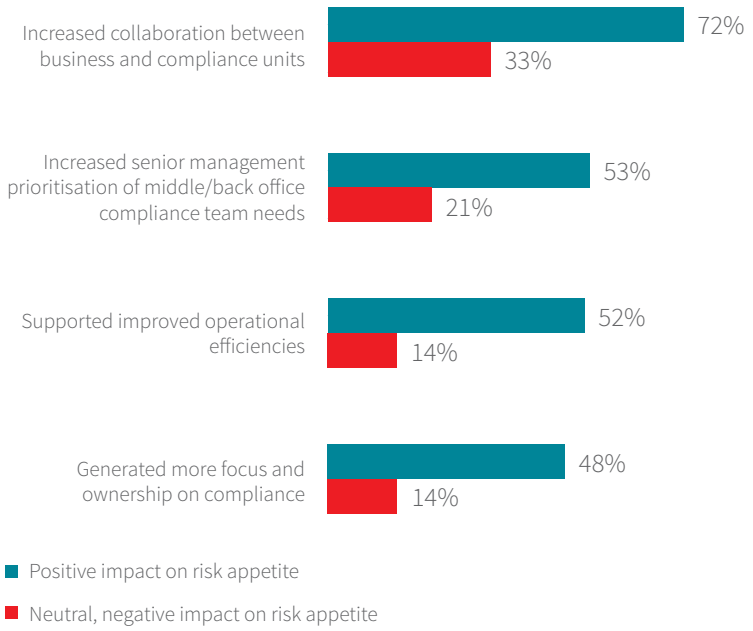


This is closely related to experience. Those who said it has had a somewhat or significantly positive impact were more likely to have experienced the benefits of increased collaboration, senior management prioritisation, operational efficiencies and shared risk ownership. In essence, these benefits have made those organisations feel better equipped to address risk.

Figure 10

Q. Which of the following, if any, are ways that the SMR has made an impact on your organisation? (Respondents could select more than one option; n = 168)

Top mentioned SMR impacts on organisations



2.2 Tell me when to stop...

"We're aware that there are things we need to comply with, but we're not entirely sure what we need to be complying with first ..."

Whilst acknowledging the positive aspects of increased liability, there are points of confusion that still exist, particularly around lack of clarity and guidance in relation to what actions, or lack thereof, are liable to land individuals in trouble. As one professional noted, *"It's not a clear picture of what passes the threshold of being personally and criminally liable. You don't know which thing that isn't paid any attention to is the one that causes you to get into trouble".*

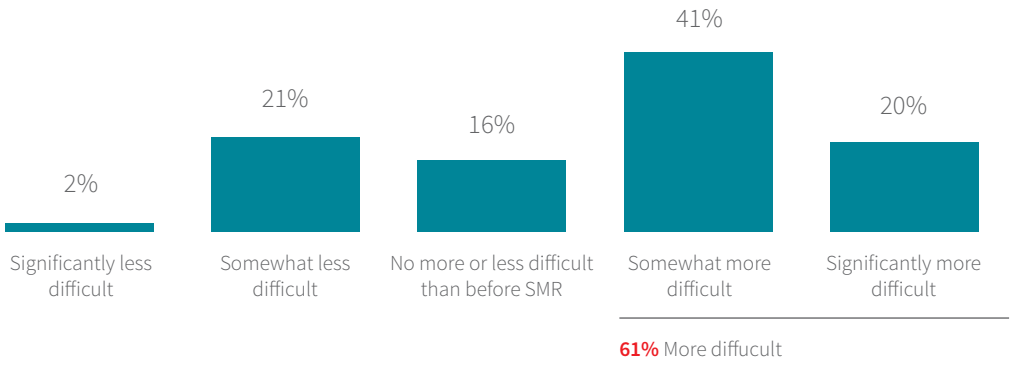
As a result, many transactions get higher levels of scrutiny than they otherwise would or should, resulting in over-reporting of SARs and micro-management. This, in turn, creates "box ticking" compliance behaviour at the expense of proactive financial crime fighting – which is exactly what the FCA publicly states it doesn't wish to have happen[9]. One financial crime expert summed up the irritation, *"I complain about checking off the boxes all the time. But I get quite excited when somebody actually wants me to do something about fighting financial crime".*

Survey respondents were more likely to tell us that their job has become at least somewhat more difficult since the introduction of the SMR – the result of increased paperwork and documentation. Anxieties caused by this may not permeate all levels of financial organisations. Many financial crime professionals that we spoke with indicated tensions are more pronounced among those new to this level of accountability (i.e., 1st line of defence) and business heads / senior executives as attestations have increased. Money Laundering Reporting Officers (MLROs) had this degree of responsibility long before the Senior Managers Regime.

Figure 11

Q. With the SMR placing more accountability on the business itself, what impact if any has this had on your job in terms of difficulty? (n = 168)

Impact of more accountability on job



For those new to the responsibility, it may not yet be entirely clear that significant liability occurs from egregious or wilful error (or both). Such tensions may ease as it becomes more widely understood, newer processes are put in place and people become accustomed to increased accountability.

9. Speech by Megan Butler, Executive Director of Supervision - Investment, Wholesale and Specialists at the FCA; "A More Effective Approach to Combatting Financial Crime" delivered at the BBA Financial Crime and Sanctions Conference and published 21 September 2016 (Updated 29 September 2016); "We do not want you to take, and I know from speaking with firms that you don't want us to take, a 'tick-box', legalistic approach to financial crime compliance in the UK" https://www.fca.org.uk/news/speeches/more-effective-approach-combatting-financial-crime

2.3 It's always better the second time around...

"I don't think the reality has been the same as the expectation."

This title is a very different tone than reported in our 2015 report, which was prior to the Senior Managers Regime coming into force. At this time, we reported that up to 60% of survey respondents would choose a career path other than financial crime compliance in light of increased personal liabilities (54% would choose another path, 6% might choose another path).[10]

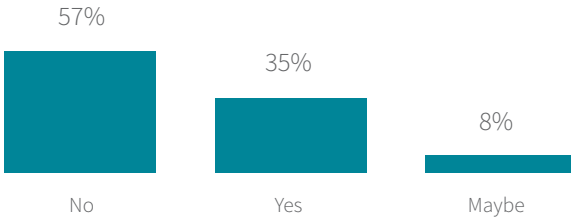
Some of this could have been related to having the same level of risk responsibilities without commensurate pay as others; *"I can assure you I do not get paid at the same level... pay should be commensurate with risk."*[11] But nonetheless, it ultimately related to increased personal risk.

Following the SMR's first anniversary, a different tone has manifested. The 60% who would not choose a financial crime career again has dropped to 43% (35% would choose another path, 8% might choose another path). Despite increased difficulties, there is also recognition of the benefits of heightened accountability and an understanding that this is indeed manageable.

Figure 12

Q. If you had the opportunity, would you choose a career path other than financial crime compliance, in light of the increased regulatory pressures? (n = 168)

Likelihood of choosing a career path other than financial crime compliance, in light of the increased regulatory pressures.



Financial crime professionals that shared their opinions and insight also said that more personal accountability hasn't impacted their ability to fill positions or retain employees. As one interviewee observed, *"This time last year I would have definitely said this will make people avoid or leave these jobs. But I'm not sure it has, to be honest. I've seen a number of MLROs in the UK appointed, take jobs, big jobs, who are really good people. So I don't think the reality is – has been the same as the expectation."*

In addition, very few survey respondents this year indicated that the SMR had made it challenging to hire people for positions for which they will be held liable (only 13%), created more staff turnover (only 16%) or even created more stress among the first line of defence (only 9%).

10. 2015 Future Financial Crime Risks, a LexisNexis Risk Solutions report produced for the BBA, November 2015
11. Ibid

Looking forward, some financial crime experts told us they expect more prosecutions over the next year, which can provide more clarity around what actions (or lack of) are likely to lead to prosecutions and further reinforce the focus on prioritising compliance. *"I think the biggest impact will be as we start getting individuals being prosecuted for actions they've taken - then you'll see a mind change or certainly a focus on risks and potential resourcing to prevent that risk or to mitigate that risk."* As another said, *"In the next year or so, the MLRO community will have accepted that they're going to have to do something reckless and egregious and negligent before they go to jail. Which should clear things up a bit".*

Observations of LexisNexis® Risk Solutions

Staff shortages

Hiring experienced financial crime professionals is an increasing challenge for UK banks. Salaries to attract the right talent are high and competition between financial institutions is fierce. As such, providing an interesting and challenging work environment and positioning the existing talent an organisation has in the place where they will have most impact is critical. Workloads need to be prioritised effectively, so that the right resource is working on the right thing. More intelligence is needed as the risk based approach advocated by the 4th Anti-Money Laundering Directive leads organisations to have to enhance their compliance skillsets.

The hope is that automation via artificial intelligence and machine learning will take up the bulk of the lower risk, higher volume cases managed at one end of the scale. Leaving the high risk, lower volume cases to be managed by the most experienced financial crime compliance professionals at the top of the chain; effective resource allocation will ultimately support effective financial crime prevention.

Simultaneously, the development of the next generation of financial crime leaders, by those currently in senior positions, is critical to the defence of financial services and the economy as a whole. The lack of clear succession planning, could itself be considered a future financial crime risk.

Business engagement with the compliance function

Increased collaboration between the front office and compliance departments will create a variety of benefits. In addition to generating a better understanding and increased accountability for compliance requirements, it presents an opportunity to empower those front line staff and improve both the customer experience and first line of defence in an effective compliance culture; bringing compliance as close to the client as possible will have major benefits. It seems the Senior Manager Regime has helped this evolution despite previous concerns.

The net result? Front office staff are able to expedite customer on-boarding, whilst compliance staff are focusing on cases which genuinely need their attention and the customer enjoys a frictionless experience.

3. Cost of Compliance

Key Findings

- **Regulations & complexity:** Greater regulation and increasingly complex criminal methods have driven up compliance costs.
- **People & technology:** Resource hiring and legacy technology systems are key cost components.
- **Specialisation:** Mass recruiting looks to be over; now is the time of the senior skilled specialist, which further drives up salary demands.
- **RegTech alternatives:** RegTech companies could be the answer to costly legacy system upgrades and overhauls.

Respondents told us that the cost of compliance for UK banks continues to rise and is a significant issue. Nearly two-thirds indicated that costs had been increasing over the last 2 years, with retail / wholesale banks particularly experiencing this trend.

Figure 13

Q: What has been the trend with the cost of compliance in your organisation over the past 2 years? (n = 168)

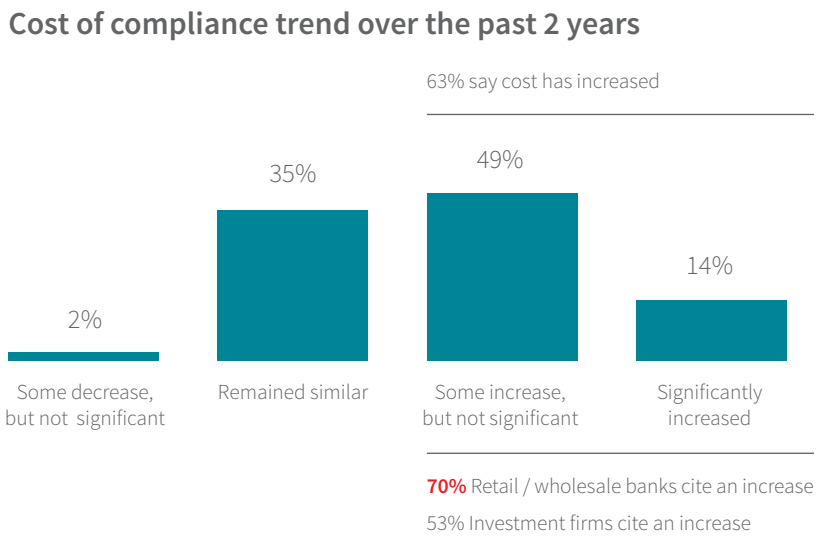


Figure 14: Cost factors that emerged from research interviews

Cost of compliance factors

Human Resources

- Increased Hiring
- Increased salary demands

Technology

- Legacy system expenses
- New solution investments

Breaches

- Significant fines for non-compliance
- Significant legal fees for non-compliance

Data

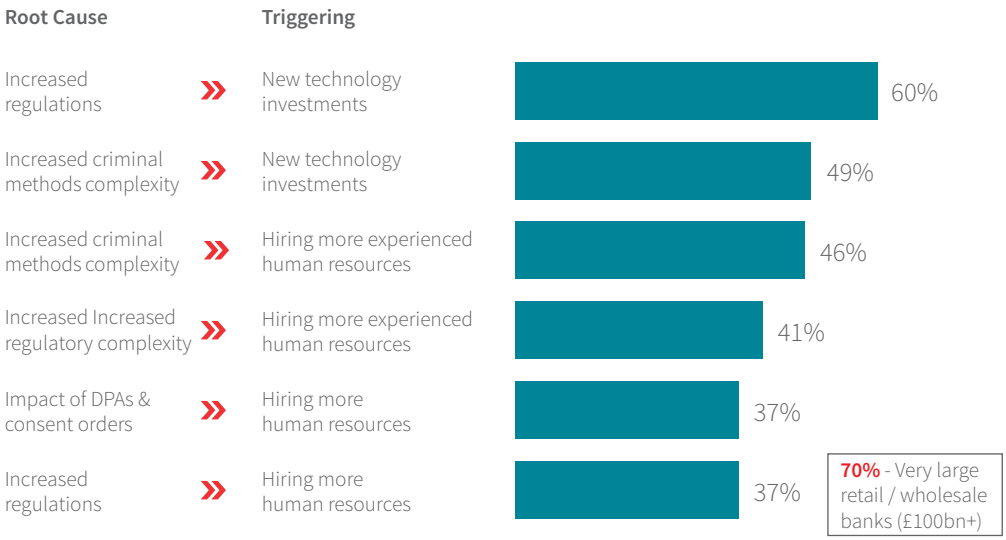
- Big Data to develop fuller profiles of clients
- Deeper data to understand relationships and assets

These, however, are only factors which increase cost; they are not root causes. Those lie squarely in the increased regulatory requirements and complexity of criminal methods, which drive the need for additional technology investment, specialised resource spending and general hiring.

Figure 15

Q: Which of the following have been root causes of the increased cost of compliance in your organisation? (Respondents could select more than one option; n = 168)

Root causes of compliance cost increases



3.1 Nothing in this life is free... Part I

"You have to spend as much as you need to get it right..."

"I've never in 20 years seen the volume of regulatory change we're seeing in the financial crime arena. This and the broader change in terms of structural reform... banks are having to spend more and more money".

Investment in new or enhanced technologies tops the list (60%) of cost triggers based on increased regulations as a root cause. A number of specific technology costs contribute to the overall rise

Figure 16: Specific technology costs mentioned during research interviews

Technology cost factors

Aggregation of data from disparate systems

Implementing alternatives to data queries due to older systems not designed to support such functionality

Full optimisation of solutions to address changing criminal methods

Need to reduce manual labour hours and resource wastage

Some of these issues are due to past mergers or acquisitions, where banks inherited systems that were different from their core systems; but the technology pain is shared across banks, large and small – regardless of past M&A activity or not.

Ongoing patchwork upgrades can add to operational and risk management costs. All financial firms need to continue investing in technology to keep up with, and hopefully ahead of, changing criminal methods. As one financial crime professional said, *"you have to spend as much as you need to get it right or decide to go out of business. There is no alternative".*[12]

Concerns about compliance costs have not gone unnoticed by the Financial Conduct Authority (FCA). In November 2016, Rob Gruppetta, Head of Financial Crime at the FCA, told an audience at the FCA Financial Crime Conference that the regulator wishes to support ways for the finance sector to reduce the cost of compliance. Megan Butler, Executive Director at the FCA, has also acknowledged the impact of compliance costs by saying *"we do not want a future where efforts to tackle financial crime are put back by disproportionate procedural compliance costs".*[13] She went further to promote technology innovation, RegTech (Regulatory Technology) teams and the FCA's Sandbox scheme as opportunities for addressing this issue.

12. Speech delivered by Rob Gruppetta at the Annual AML & Financial Crime Conference; http://www.law360.com/articles/863121/5-questions-about-the-fca-s-big-financial-crime-push
13. Speech delivered by Megan Butler at the BBA Financial Crime and Sanctions Conference, 21 September 2016; https://www.fca.org.uk/news/speeches/more-effective-approach-combatting-financial-crime

In our interviews with financial crime professionals, a few mentioned that RegTech firms may be the "on the horizon" alternative for those facing costly updates or replacements of legacy systems; as explained by one interviewee, *"RegTech gives us an opportunity to design a system in isolation of a significant contractual agreement".*

Others, however, noted that the financial sector is just *"beginning to get our heads around the RegTech side and the advantages technology can bring to the compliance world".* To fully leverage the opportunities which RegTech can convey, it may be necessary to recruit talent with alternative skills to complement the traditional investigative and legal skillsets of financial crime professionals. Individuals with a technology or data analytics background are likely to come into demand as the industry turns to RegTech for solutions; indeed this is already happening as one respondent from a major multi-national bank highlighted they had hired *"Half techie, half financial crime"* talent.

3.2 Nothing in this life is free... Part II

"We have to hire more people. If we have to hire more people, that's more cost."

Human resource requirements, both permanent staff and contract workers, continue to be a significant cost factor. Survey respondents confirmed this; almost half (46%) of those citing increased compliance costs pointed to the need for hiring more experienced human resources. Very large retail / wholesale banks (£100bn+) were significantly more likely than others to have said that increased regulations have resulted in the hiring of more human resources in general.

The introduction of Deferred Prosecution Agreements (DPAs) in 2014 has contributed to some of this hiring. DPAs are a double-edged sword; they offer deferred prosecution but to achieve this organisations must meet a variety of deadlines and requirements, such that banks need to assign a multitude of resources – hence overtime hours, new hires and more cost as the fastest way to remediate and comply.

A leading recruitment firm has reported that the need for "financial crime professionals was a consistent requirement for companies in 2016".[14] But there appears to be a shift from mass hiring to more specialised recruitment. Some major UK banks increased staff significantly in 2013[15] – 2014[16] to deal with increased regulations and DPAs. During recent interviews, there was mention that bulk hiring may be over as banks come out from under these deferred agreements. Instead, hiring is focused on those with specialised or "permanent" skills.

14. InCompliance magazine, International Compliance Association – Looking back, looking forward, article by MorganMcKinley; https://www.int-comp.org/media/4143/pages-from-march-2017.pdf
15. JP Morgan hired 4,000 in 2013 to deal with compliance; http://www.lexology.com/library/detail.aspx?g=48148a7f-9c22-40de-ac4f-67ec0d4dd10e
16. 2,157 new UK specific AML roles were created in 12 months to August 2014; http://www.brightpool.co.uk/additional-information/jump-in-demand-for-anti-money-laundering-expertise-as-banks-face-increased-scrutiny-from-fca/

This opinion is supported by a leading recruitment firm which noted that ''the demand for candidates with a generalist background decreased throughout 2016", a trend they anticipate continuing in 2017, as the need for professionals with specialised skills increases.[17] In particular, it highlights that individuals with investigation experience are desirable "as they have the necessary investigative skills to produce high quality written risk assessment reports".[18]

This sentiment was echoed in the comments made by one senior banker, *"the knee-jerk reaction to build on was done, and there's going to be people looking for work. The bits that are resilient to that downward effect are going to be those people that have built up their specialist skills for their specific niche areas."*

More specialisation often demands higher salaries, particularly if many banks are competing for the same, limited resource pool. Average reported salaries from a leading recruitment firm show strong increases from 2015 to 2016, [19]at rates above the average wage increase of 2.6% – 2.8%.[20]

Figure 17: Average salary changes for Compliance and AML professionals in the UK 2014 - 2016
* Salaries are UK-wide (London specific could be higher)

	Average Salaries*			2014-15% Change in Average Salary	2015 UK Average Salary Increase	2015-16% Change in Average Salary	2016 UK Average Salary Increase
	2014	2015	2016				
Head Compliance	£145,375	£150,625	£158,000	3.6%	2.6%	4.9%	2.8%
Compliance Manager	£78,875	82,750	£82,000	4.9%	2.6%	-0.9%	2.8%
Compliance Analyst	£50,125	£52,625	£55,875	5.0%	2.6%	6.2%	2.8%
Head AML/FC Manager	£142,125	£145,500	£152,500	2.4%	2.6%	4.8%	2.8%
AML/FC Analyst	£90,875	£92,625	£97,250	1.9%	2.6%	5.0%	2.8%
AML Analyst	£49,125	£50,250	£52,750	2.3%	2.6%	5.0%	2.8%

17. MorganMcKinley 2017 Compliance Salary Survey Guide https://www.morganmckinley.co.uk/article/2017-compliance-salary-survey-guide
18. Ibid
19. Robert Half Salary Guides 2015, 2016, 2017; https://www.roberthalf.co.uk/
20. http://www.economiccalendar.com/2017/01/18/uk-average-earnings-growth-strengthens-to-2-8-brexit-debate-dominates/

Skills in demand for 2017 include regulatory awareness, transferable due diligence, experience with regulatory (FCA) correspondence and an ability to influence the compliance culture throughout the organisation. Key positions in demand, meanwhile, include compliance officers/managers/heads, financial crime specialists for KYC / AML, and model risk specialists. Putting costs aside, the positive angle is that banks who hire more specialised professionals should be in a better position to deal with anticipated new regulations, their implementation and emerging criminal threats.

Of course calculating the actual cost of compliance can be difficult. There is a quantifiable nature to all of the factors discussed above, but there is also the cost to one's brand reputation if deficiencies are publicised or if a bank becomes so prescriptive that conduct risk damages client relationships. One interviewee summed it up as *"there is a whole raft of different areas... which add to the cost of compliance. I don't think it's a calculation that says our cost of compliance is £735 million - because cost of compliance can also be reputational risk... if something goes wrong. So you can never judge that as a cost but clearly there is a cost there".*

Observations of LexisNexis® Risk Solutions

A clear line of sight

Not having a holistic view of a given customer and effectively utilising the data and intelligence available reduces the ability to make insightful decisions and significantly drives up the costs of maintaining that customer relationship. Assessing risk, categorising customers and making due diligence decisions on only a subset of the available data, can ultimately result in too much due diligence – or not enough – being conducted. Mistakes will be made.

Being able to have a quick, accurate, complete view of a customer is critical in the speed of response needed to differentiate the business and comply with customer demands.

Can automation solve HR challenges?

When challenges occur, 'throwing people at the problem' is often adopted in the first instance, with head count and costs quickly escalating in order to remediate problems. Escalating HR costs can form a significant part of the cost of compliance and often are a very short term resolution to a complex, evolving long term problem. However, this is simply throwing money at the wrong solution.

As previously described, analysing existing data, systems and processes, and optimising them, can help to reduce remediation costs and processing times, increase throughput (without hiring more people) and create a more effective means of preventing financial crime over the long term, driving improved results.

4. De-Risking

Key Findings

- **Case-by-case** exiting has replaced wholesale de-risking.
- **De-risking is considered a legitimate** and prudent commercial decision.
- **Banks want further clarity** and guidance from Regulators.

4.1 What's in a name?

"De-risking is a pejorative term..."

Cost of compliance has also emerged as one factor driving the exiting of client relationships. But it isn't the only factor; there is also AML compliance. As the FCA has mentioned that "banks are withdrawing or failing to offer banking facilities to customers in greater volumes than before... influenced by big fines... [for] weaknesses in their anti-money laundering defences",[21] UK banks are quick to point out that measured, case-by-case exiting of relationships linked to or suspected of financial crime is in fact a duty prescribed by the FCA. In other words, it's perfectly legitimate and required under the principles of compliance.

Many banks in our study even objected to the term by which exiting is commonly referred to - "de-risking". It is perceived as carrying negative connotations of wholesale exiting of markets or lines of business which occurred in the recent past.

UK banks recognise the negative consequences that resulted from that, and there is now consensus that client exiting must be done on a case-by-case basis. *"Well... it's been challenged... and we all agreed as an industry that de-risking of whole sectors is not an appropriate response"*, said another respondent from a leading bank.

In essence, client exiting decisions now have wider factors driving them. Whereas previously the main drivers could be linked to pure risk aversion, increasingly the decisions are based upon business reasons beyond money laundering or terrorist financing risk alone.

Putting compliance and financial crime aside, "client-exiting" is viewed by banks as sound commercial decision making. All businesses need to remain profitable; if it costs as much (or more) to conduct due diligence on a customer than the value of the relationship itself, one can argue that this dictates exiting is basic business practice. If that client is also part of a jurisdiction, sector or business line of higher risk then the cost of compliance combined with risk makes exiting an even more prudent commercial decision.

> " I don't like the phrase de-risking. Strategically you should look at your client base, and anything that is either not profitable, that's inactive, or where the cost of compliance isn't good, then you should be able to get rid of it."

21. https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking

The FCA has acknowledged this in reference to its 2015 research "Drivers & Impacts of De-Risking" (the Howell Report), citing that *"firms we regulate have commercial freedom, subject to some restrictions, to choose who they do business with. Banks have always had to make decisions about whether or not to provide their services to a prospective customer, or maintain a relationship with an existing customer... [based on] potential credit risk and profitability of a relationship, concerns about the reputational consequences of providing services to certain customers"*[22]

4.2 Not so fast... It's not that simple

"You'll be second-guessed if you're not careful..."

The matter of closing client accounts, for various reasons and whether one calls it "client exiting" or "de-risking" is not that simple. Whether a firm is exiting clients because of suspected financial crime risk, potential credit risk or lower cost/benefit reasons, the current regulatory and legislative environment can be difficult to navigate.

In some cases, laws and regulations can pit different objectives against one another.

POCA (Proceeds of Crime Act) - Once any higher risk customer has been identified, the potential additional due diligence and monitoring required on those accounts will add to the cost of compliance, which in turn could lead to the closing of less profitable accounts.[23]

- If suspicion has been raised during monitoring, then an investigation must ensue, the account is then suspended and the bank is restricted from explaining its intent based on the "tipping off" offence in section 333A of POCA.
- Where this creates public debate with the client, it can lead to reputational risk, particularly involving high profile clients.[24]

PEPs and the Bank of England and Financial Services Act 2016 The FCA will now potentially have authority to penalise financial firms for doing too much due diligence where politically exposed persons (PEP) and their family members or close associates are identified as well as being able to penalise for too little due diligence. This feels like a Catch-22 to some with whom we spoke; *"So now you'll get fined at the top end of the scale and the bottom end of the scale. So if you do too much due diligence, you'll be fined. If you do too little, you'll be fined."*

There is a balancing act which banks must observe with regard to "de-risking" and their position in the marketplace. This relates to "abuse of dominant position / market power" and an infringement of competition law as contained in the UK Competition Act 1998 and Treaty on the Functioning of the European Union[25]

22. Ibid
23. http://www.lexology.com/library/detail.aspx?g=48148a7f-9c22-40de-ac4f-67ec0d4dd10e; Is De-Risking an Over-Reaction to Over-Regulation, 24 August 2016
24. Ibid
25. http://www.compliancemonitor.com/uk-regulation/Competition/do-fca-de-risking-warnings-raise-more-questions-than-they-answer-119292.htm; Do FCA De-Risking Warnings Raise More Questions Than They Answer, 7 September 2016

- A financial institution could be exiting a relationship based on any of the previously mentioned decision factors; but if that leads to cases of restricted competition within the affected client's sector or an advantage for the bank itself, then this could be prosecuted as violating competition law. This recently occurred in the case of a Money Services Bureau (MSB) account being terminated, even though that client was clearly transferring funds to a terrorist-controlled region.[26] Furthermore, financial institutions need to be wary about perceptions of being in collusion with each other that leads to their collective advantage.

Banks are required to manage risk yet financial crime concerns are being fettered with new regulations that can lessen their control.

- The Basic Payment Accounts Regulations 2015 which came into force in September 2016 make it mandatory for UK banks to offer at least a basic payment account to consumers who apply on or after 18 September 2016; it will further restrict the ability for banks to terminate such basic payment accounts.[27]
  - » This makes it easier for criminals and terrorists while adding more work for financial firms to monitor and assess risk that they might have otherwise shut out at the beginning.
- The Second Payment Services Directive (PSD2) will add to this at least as long as Britain remains in the EU – or keeps this directive after completion of Brexit.
  - » Article 36 of PSD2 incorporates a section entitled "access to accounts maintained with a credit institution", which indicates that banks must provide "reasons for rejection" to regulators and that de-risking shouldn't be one of them.[28]
  - » PSD2 also means that UK banks need to provide access to customer data to Fintechs and challenger banks, which opens up further security and risk concerns.

Whilst there are good policy reasons for the above legislation, throughout our discussions, a common theme was the need for stronger guidance from the FCA on many areas of compliance. "De-risking" is certainly one of them, especially as newer regulations will likely continue in this hyper-scrutinised environment.

And whilst the FCA has issued various types of guidance, the industry believe there is more that can be done. As stated by a senior banking official, *"I think FCA guidance definitely has impacted things. It's really hard, from a regulatory perspective. I think regulators try hard. They're in an incredibly difficult position. I think they do tend to apply one size fits all, which is wrong, actually. So that's something they're going to have to think about."*

4.3 Guess who's coming to dinner...

"You don't exclude everyone... but you don't take everyone either..."

None of this is made any easier for banks and regulators when taking a practical, unfiltered look at segments which have historically been more prone to high risk and account exiting / exclusions. The FCA's report points to the following segments as typically being impacted by de-risking.[29]

26. Ibid
27. http://www.lexology.com/library/detail.aspx?g=48148a7f-9c22-40de-ac4f-67ec0d4dd10e; Is De-Risking an Over-Reaction to Over-Regulation, 24 August 2016
28. https://www.law360.com/articles/829045/uk-regulators-worry-de-risking-has-gone-too-far
29. https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking

Figure 18: FCA-reported segments typically impacted by de-risking

Which segments are typically impacted by de-risking?

- Money Services Bureaus (MSBs)
- Charities
- Financial Technology Companies (Fintechs)
- Correspondent banks

There are, however, some valid reasons for placing more attention on these types of organisations, including but not limited to:

Figure 19: Reasons for concern about certain types of organisations

Why are there concerns about these organisations?

- Not being bound by the same rules and regulations as banks
- Having clients who may, for various reasons, be ineligible to hold a bank account (MSBs)
- Lacking transparency into transaction details: limited visibility into their customers (MSBs, correspondent banks, charities)
- Operating in higher risk locales

One financial crime professional commented *"Why are people worried and scared about banking MSBs? It's because they're not bound by the same rules and regulations, and because they have sub-agents and further agents and further agents, and there has been a lot of negative press in relation to the booking and records."*

If there is risk aversion based on locale, it is common sense to say that concerns are heightened by the other due diligence blind spots mentioned above and that the cost / return value of determining this on an ongoing basis may outweigh the decision to remain. This is not an attack on whole sectors themselves, but an acknowledgement that higher potential for risk requires more due diligence and costs, and that there are times when banks need to do what is required as a result; to exit or refuse an account based on either risk or commercial profitability.

As another banking professional put it, *"You don't look to exclude everyone, because that's lost business... lost good business. So say for instance, if you were banking such and such MSB, and that's a perfectly good legitimate business as an example, compared to a Mickey Mouse version, you're not going to apply a single blanket approach here. That isn't sensible."*

This line of commercial thinking may also extend to Fintech companies. Not that they are bad per se; instead, it's quite possible that being newer to the game requires more time for both understanding and acceptance. Fintechs may be having more difficulty establishing relationships with banks from a commercial value perspective than actually being "de-risked".

As stated during our interviews, *"I think it's not so much a big de-risk. I think they're finding it hard to get relationships to begin with, because they're new and they're bright and they're emerging. How much time and cost does it take for a bank to do its due diligence to see whether they're one of the good guys or one of the bad guys? That takes resources. For a bank like us, it is more likely that we'll wait until somebody else has invested in them before we buy the whole thing."*

Correspondent banking is another sector under the regulatory microscope, which has been experiencing decline for different reasons. The first is a reduction in the number of correspondent relationships that banks have, because of either commercial value or risk; another is a changing focus among some banks to more traditional correspondent methods that support cross-selling to each other. Some are also reluctant to continue supporting certain foreign currencies or geographic locations.[30]

Whatever the reason, it has attracted the attention of regulators and government bodies. The Financial Stability Board (FSB), an international body of regulators, has included correspondent banking in its four-point plan to better understand the root causes of its decline and to use those insights in policy initiatives to turn this trend around.

The Financial Action Task Force (FATF), an inter-governmental body which develops and promotes AML / anti-terrorism financing policies, has made recommendations to alleviate banks' concerns about correspondent banks' customers; "financial institutions should not be required to conduct customer due diligence on the customers of their respondent bank clients (so-called "know your customer's customer")".[31] The FCA appears to support these efforts.[32]

It is perhaps too early to tell what the trend will be in the next 24 months in correspondent banking but it will clearly be based on such efforts. Will these alleviate concerns or address the real drivers? Will they change the profitability equation that underlies commercial business decisions regarding client relationships?

The latter point may well be the deciding factor. As one financial crime interviewee pondered, *"So every single correspondent banking relationship you have, you're expected to treat them as high risk, do loads of extra work. If you have 1,000 of these relationships, and half of them you use very little, why are you going to be spending a bum maintaining those relationships? There's probably only two, maybe three banks who really connect everything together, but then all the other banks have to have nostro and vostro accounts so that they can then be connected to the international trade."*

30. Ibid
31. http://www.fsb.org/wp-content/uploads/FSB-publishes-progress-report-and-2017-workplan-to-assess-and-address-the-decline-in-correspondent-banking.pdf
32. https://www.fca.org.uk/news/statements/we-support-financial-action-taskforce-work-de-risking-drivers

On a positive note, though, the FCA seems to recognise the complexity of challenges related to client exiting. It has said that no "silver bullet" exists to the set of complex drivers of "de-risking".[33] But it does point to the recent Payment Accounts Regulations and the 2nd Payment Services Directive as ways that are hoped to help some sectors impacted by "de-risking".[34] The FCA has also put de-risking squarely on its 2016/2017 Business Plan, with reference to ways that new technology might help AML processes become more efficient and "reduce financial exclusion".[35]

Observations of LexisNexis® Risk Solutions

Informed decisions

The availability of and access to the right information is often cited as one of the key challenges which drive financial institution's de-risking decisions. Missing and incomplete data can make it difficult to ascertain the risk associated with an entity or significantly enhance the cost associated with this business.

By removing internal data silos and drawing upon reliable external information, a clearer understanding of the risk a relationship presents can be attained. In addition, utilising technology to analyse this data and drive decisions will ensure costs are kept to a minimum which may not result in an exiting decision and ultimately promote greater financial inclusion and competitive differentiation.

Manage the risk – manage the crime

Managing risk has become an increasing challenge for the regulated Financial Services sector. How to safeguard the financial system from illicit monies and detecting it if it does make it in, is somewhat of a Holy Grail.

Yet there has always been risk in the system and a degree of illicit funds flowing. Controversially it could be viewed that it is better if banks and regulators use their compliance expertise to maintain some level of risk on the books. Money, criminal or otherwise, will always flow, and if it's not held in the mainstream, it will disappear into shadow banking channels or other areas of the economy with little to no visibility, making it even more difficult to combat financial crime. The emergence of digital currencies and online payment systems over the last ten years has added to the challenge. Consequently, smarter, faster systems and intelligent assessment of information is becoming crucial.

It is clear, that the conventional financial system is best equipped to manage this risk by making better use of the systems, data, intelligence and expertise available. The key to achieving desired outcomes is the management of such risk as opposed to total avoidance and de-risking, but this must be conducted in the right manner with legislation to support the process of investigation leading to outcomes, underwritten with appropriate protections for both professionals and institutions.

33. Ibid, https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking
34. Ibid
35. https://www.fca.org.uk/business-plan-2016-17/3-our-priorities#op2

5. Technology & Financial Crime

Key Findings

- **The effective deployment of technology is not keeping pace** with financial crime and could ultimately become a barrier to fighting it.
- **The FCA is championing innovation** in technology.
- **RegTech firms could provide an alternative** to legacy technology.
- **Continual hiring of human resources** will start to achieve diminishing returns and is not a scalable and effective long term way to prevent financial crime.

2016 saw the FCA champion innovation in technology. Project Innovate saw the introduction of the Regulatory Sandbox which provides organisations with a "safe environment" to test new ideas,[36] and a firm nod was given to the potential that distributed ledger technology and blockchain application could provide to UK banks.[37]

The FCA has also has been working with RegTech firms to explore ways in which technology can be implemented and utilised more cost effectively by UK banks. A position reflected in a speech by Christopher Woolard, Director of Strategy & Competition at the FCA, during a speech at the BBA FinTech conference in September 2016:

> " RegTech has the potential to free up large sums of operational and capital expenditure which are currently spent on compliance. This potentially increases firms' capacity to innovate."

5.1 Technology can be our friend... or enemy...

"Not sure that technology is keeping pace with financial crime..."

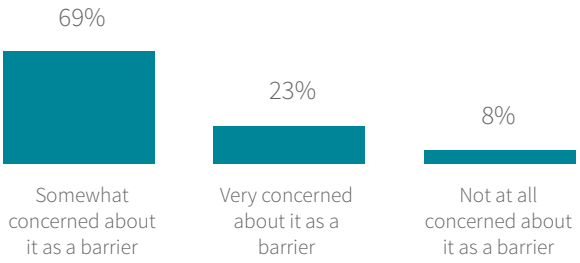
Many UK financial firms acknowledge that their existing technology is a challenge to fighting financial crime. Nearly all (92%) survey respondents expressed having at least some concern that their legacy technology could become a barrier to this effort over the next 1 – 2 years.

36. From speech by Christopher Woolard, FCA Director of Strategy & Competition, at the BBA's FinTech Conference September 2016; http://www.mondovisione.com/media-and-resources/news/the-fcas-role-in-promoting-innovation-speech-by-christopher-woolard-director/
37. Ibid

Figure 20

Q: How concerned is your organisation about the impact of legacy technology as a barrier to fighting financial crime during the next 1 – 2 years? (n = 168)

Concern about legacy technology impact on fighting financial crime



Various challenges exist, including:

Figure 21

Q: To what degree are the following a challenge for your organisation with regard to technology when fighting financial crime? (Respondents could select more than one option; n = 168)

Technology challenges when combatting financial crime

41% say ability to keep pace with changing criminal methods

39% say expense of new technology solutions

37% say technology location that could inadvertently cause compliance breaches

53% large retail/wholesale banks say frustration of multiple systems across various jurisdictions

Financial crime professionals also pointed to concerns that inefficiencies / gaps in data gathering could prolong risk exposure and investigations, impede current relationships and create complexities requiring additional human resources.

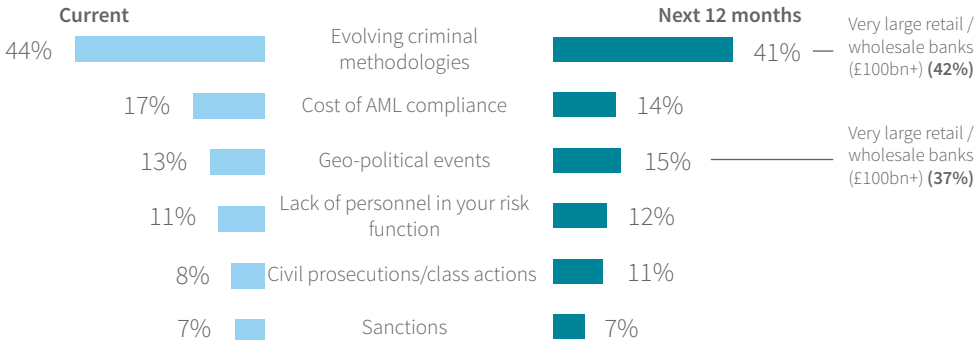
At the same time financial firms recognise these technology concerns, they see real threats and worry about not being fully prepared to address them. Evolving criminal methodologies continue to remain the single biggest financial crime risk for them; nearly half (44%) said this in our 2015 report, the same percentage said it is the biggest risk today. 41% say it will continue to be so in 2017.

Very large retail/wholesale banks, particularly, expect to juggle this plus the impact of geo-political events in the near-term. This indicates that the industry has more work to do; it hasn't fully tackled this issue yet.

Figure 22

Q: What would you say is the biggest single financial crime risk to your business at the present time? In the next 12 months? (n = 168)

Biggest single financial crime risk to the organisation



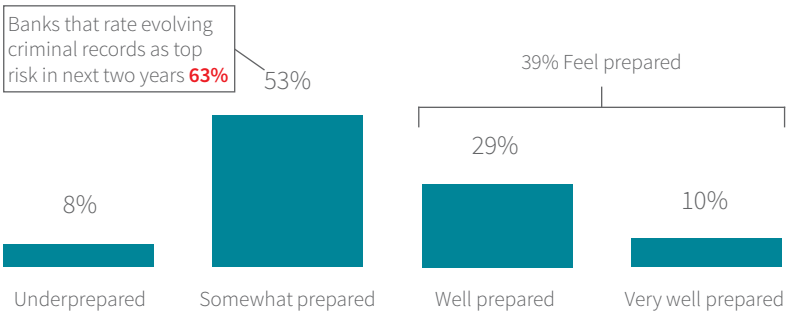
"the pace has changed in terms of technology and criminal technique – their typologies. At the same time, there's a maturity in fighting financial crime and developments like public/private partnerships and advances in technological monitoring. But, there is the political environment, which is going to throw, I believe, a lot of spanners in the works and create a very rich environment that's probably got less predictability in it than at any time over the last few decades."

Cybercrime is one of those evolving methods that has received attention in the past year. Along with regulatory pressure, this is a significant burden on UK financial organisations and a majority don't feel fully prepared to protect themselves from it. This is heightened among banks that see evolving criminal methods as the biggest risk over the next two years.

Figure 23

Q: How well prepared do you feel your business is to tackle changing criminal methodologies, such as the use of digital payment methods? (n = 168)

Perceived preparedness to protect business from changing criminal threats specific to cybercrime



Not surprisingly, over one-third (39%) of survey respondents said that cybercrime prevention will be their top investment over the next two years; this is similar to the proportion in 2015 (37%). The most concentrated segment to say this is retail/wholesale banks who see evolving criminal methods as their biggest threat; two-thirds (67%) of those said that cybercrime is their next 1 – 2 year investment priority.

This segment is more likely than others to say that banks' technology has not kept pace with advances in cybercrime (70% versus 50% amongst all respondents).

Figure 24

Q: What is your level of agreement with the following statement about technology and financial crime? (n = 168)

Banking technology hasn't kept pace with advances in cybercrime
(%Agree)

5.2 Is RegTech the future?

"We're just getting our heads around the FinTech and RegTech side..."

One obvious question is whether, as well as causing new problems, technology might also provide the solution to such challenges?

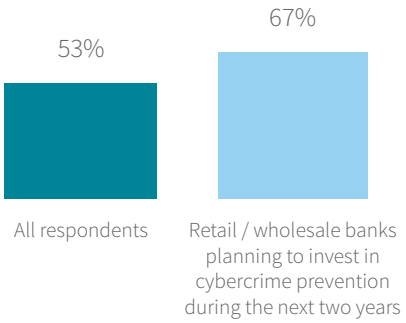
More than 9 out of 10 respondents (91%) highlighted that their organisation was concerned about the impact of legacy technology acting as a barrier to fighting financial crime during the next 1 – 2 years. It's perhaps unsurprising then that financial institutions consider RegTech (technology solutions designed to solve regulatory challenges and support compliance) as an alternative.

Just over half (53%) said that RegTech companies are the alternative to legacy systems for fighting financial crime. During our in-person interviews, it was mentioned that RegTech might also provide future opportunity for industry-shared resources.

Figure 25

Q: What is your level of agreement with the following statement about technology and financial crime? (n = 168)

RegTech companies are the alternative to legacy systems
(%Agree)



It would seem that financial services, and its approach to financial crime prevention, is behind the curve in terms of technology. RegTech can bring to bear the latest technology such as Artificial Intelligence and Machine Learning to optimise outcomes, enabling human resource to focus on areas of most impact and helping to reduce the cost of compliance through process efficiencies.

Another key benefit that RegTech offers is that it can reduce the need for wholesale change to existing systems[38]. It can address disparate data and technology challenges for the purposes of regulation and financial crime prevention. RegTech can mine existing data and utilise existing systems[39] to produce consolidated intelligence and reporting in a more cost effective manner and help avoid the need for full-scale capital expenditure.[40]

Many RegTech solutions are cloud based, resulting in solutions that should be more operationally flexible, cost-efficient (no physical infrastructure or maintenance expenses) and scalable (add to as needed). Of course, there is some debate as to whether cloud-based systems can provide the same level of security as on-premises systems, with strong arguments on both sides; and organisations do need to conduct thorough due diligence into this factor when looking to a cloud-based RegTech solution. The benefits cloud-based systems bring to businesses and consumers have recently been acknowledged by the FCA[41], but it also reminds firms of the need to comply with data protection legislation.[42]

38. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/ie-regtech-pdf.pdf
39. Ibid
40. From speech by Christopher Woolard, FCA Director of Strategy & Competition, at the BBA's FinTech Conference September 2016; http://www.mondovisione.com/media-and-resources/news/the-fcas-role-in-promoting-innovation-speech-by-christopher-woolard-director/
41. http://www.bankingtech.com/607782/fca-green-lights-cloud-technologies/
42. Ibid

A key question that financial firms will need to address is the longer-term value that RegTech solutions bring to the game. Whilst these may address the operational and cost aspects of compliance today, will such solutions also help in the fight against financial crime in the longer term? Will financial organisations be able to apply such "work around" approaches to legacy systems and get the same level of results that could be realised through making solid investments in current system upgrades and overhauls?

The answer might be different based on who you ask. For smaller firms without extensive IT infrastructure, and lacking a disparate array of inherited systems, the RegTech path could be more beneficial long-term. For larger organisations, this may not be as clear-cut, but there is certainly potential to innovate and provide a means to keep up with changing criminal methods using next generation technologies to drive both efficiencies and effectiveness.

5.3 Blockchain

In the picture, but ready for primetime?

Blockchain distributed ledger technology has been around since the early 2000s, but has attracted more interest within the financial services community in more recent years. In our 2015 report, we said that "the race to figure out Blockchain technology looks likely to be the banking industry's version of the space race" and that many global banks had already started investigating its potential use cases. That seems to still be true.

Many leading banks have begun testing Blockchain for a variety of applications. Royal Bank of Scotland, Barclays and Santander have done so for international payments.[43] Bank of America, Citigroup and others have begun testing as a means of supporting back-office cost reductions with an eye towards also shutting out cybercriminals.[44] In addition, Deutsche Bank recently moved their Blockchain project out of the concept stage and may be ready to launch in 24 months, though indicates that it will be another 5 to 10 years before widespread use given the need for "the regulatory and legal framework to deploy".[45]

But, there is already reported use of this technology. Edmonton Alberta firm ATB Financial claims to have used Blockchain to send C$1,000 to Germany's Reise Bank in late summer 2016, taking 20 seconds to complete versus days for most international bank transfers[46]. That certainly demonstrates an advantage over traditionally slower processes for international fund transfers.

Some industry analysts predict however that widespread usage could take a decade, with applications limited to trade finance rather than retail banking.[47]According to Deloitte, larger multi-national firms likely face the challenge of tackling the required "technical, organisational, cultural and talent changes" before fully implementing such a new approach.[48]

43. http://www.computerworlduk.com/it-business/how-technology-will-transform-banking-in-2017-3651834/
44. https://www.moneyandmarkets.com/banks-turn-blockchain-fight-cyber-crime-79119
45. http://www.computerworlduk.com/applications/deutsche-bank-lays-out-its-disruptive-technology-strategy-says-it-has-proven-out-use-of-blockchain-3642001/
46. https://www.ft.com/content/1b82a0e6-4f67-11e6-8172-e39ecd3b86fc
47. Ibid
48. https://www.scribd.com/doc/297275446/Deloitte-UK-Blockchain-Full-Report

Of course, there are risks associated with Blockchain; including security. Speaking at the Forrester Digital Transformation Summit in London during June 2016, Principal Analyst Martha Bennett cautioned about risk exposure based around "content on a chain [that] is clear text... easy to be decoded". She went further to add how this could create additional negative consequences if customers' personal information is breached and how that can lead to further fraud.[49]

5.4 Leveraging the advantages of technology

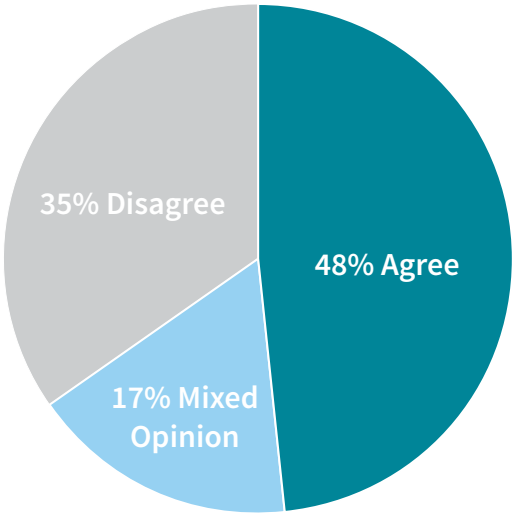
Are we doing enough?

Whilst technology investments are being made to address increased regulation and new criminal methods, financial organisations are divided on whether the industry is fully applying the advantages of technology to fight financial crime. About half (48%) of survey respondents said that the industry is not doing so.

Figure 26

Q: What is your level of agreement with the following statement about technology and financial crime? (n = 168)

Industry hasn't begun to apply advantages of technology for fighting financial crime



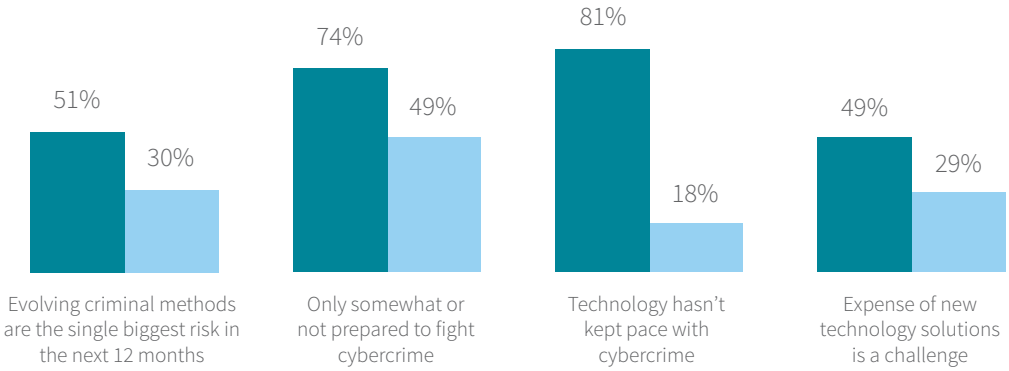
49. http://www.computerworlduk.com/data/7-reasons-blockchain-isnt-ready-for-mainstream-deployment-3641751/

The difference of opinion may lie with one's own view about challenges and financial crime risks in addition to their own understanding of technology and true advantages based on skillset. Those who believe that there is more to be done with leveraging technology benefits are more likely than others to be concerned about evolving criminal methods, feel less prepared in keeping pace with these changes and see cost as a challenge.

Figure 27

Q: What is your level of agreement with the following statements about technology and financial crime? (Respondents could select more than one option; n = 168)

An industry view of technology & financial crime



There are inevitably budgetary politics among those organisations which believe the industry isn't fully leveraging technology advantages. Where front-office management views compliance as a cost centre, technology investments have lower priority – particularly where the cost of upgrading or replacing disparate systems is cost prohibitive. The Senior Managers Regime may provide some unintended support here; as we reported earlier, it has raised senior management attention to compliance office needs.

If, however we accept that regulations will continue to increase and that there is a point of diminishing returns with continuing to just hire, or throwing more people at problems, then technology needs to be the alternative, scalable long term way to effectively detect and prevent financial crime. Combined with data and analytics-driven risk identification and management, technology can provide relief to heightened regulation, compliance scrutiny and increased personal liability.

Finally, it should be noted that existing risk management solutions don't necessarily require expensive overhauls or rewrites of legacy technology. They can integrate with and complement existing systems, delivering process efficiencies while still enhancing professionals' ability to fight financial crime by providing a clear, consolidated view of risks across the enterprise and improving process efficiencies.

Observations of LexisNexis® Risk Solutions

Technology & financial crime

Humans enabling data science

The pace of technological change continues to grow exponentially, presenting both opportunities and threats in equal measure. The criminal fraternity are early adopters of new tech to perpetrate their crimes, so keeping one eye on technology evolution is critical in order to just keep up.

Financial Crime teams have been slow to change legacy systems and adopt new technology methods historically but evolving threats, shortage of talent and the continuing drive for profitability mean this will need to accelerate to effectively fight financial crime. This transition and requirement for automation requires new skills sets such as deep technology, project management and data analytics capabilities within an effective financial crime team. Service providers must develop and commercialise systems that are robust, consistent and handle the ever increasing volumes of data being processed.

The adoption of new technologies to bring together previously disparate systems and also many different siloes of data is required to ensure both internal and external intelligence is utilised effectively. New technologies such as Blockchain, Artificial Intelligence (AI) and Machine Learning (ML) also have key roles to play in effective automation ensuring better results are delivered. In the short term these technologies will never replace what experienced human investigators and experts can do but they will ensure their time is used more appropriately. Financial Crime teams will become more effective as humans and technology begin to work together better.

6. Brexit & Geo-Politics

Key Findings

- **Brexit isn't the current primary concern within the financial crime compliance community** many of the standards are driven at an international level as opposed to EU level.
- **The Trump administration was more of a concern** regarding sanctions than anti-money laundering.
- **Neither is a significant upset to financial crime fighting:** Overall, those surveyed felt that neither Brexit nor the new American administration will significantly upset the fight against financial crime.
- **Better information sharing opportunities:** Half or more survey respondents expect that Brexit will improve information sharing between the UK and other non-EU jurisdictions.
- **More accountability and strength:** Nearly half also feel that Brexit will make the UK more accountable and give it a stronger international voice in terms of the fight against financial crime.
- **But potentially more crime & friction:** A sizeable minority expect some negative impacts from Brexit, whether from increased crime or less cooperation between the UK and EU.

2016 was a year of unexpected outcomes, from Brexit to the US general election. 2017 is also contributing its own political curveballs, with the announcement of a snap UK General Election on 8th of June.

When we surveyed financial crime professionals in UK banks (pre-UK General Election announcement), there was an underlying tone of tension; a feeling of uncertainty as to what's around the corner with global banking. This wasn't necessarily about Brexit. Instead, it was about uncertainty from the other side of the Atlantic with an American administration that is viewed as unpredictable.

Our first interviews were conducted the week following the US election. Brexit was still an issue where banks were waiting for further clarity from the Government, but there was an even-tempered mood about it overall – perhaps with some slightly positive expectations.

On the other hand, the discussion in regards to the incoming Trump administration generated more animated reactions. Could it trigger a wave of extreme nationalist outcomes in some upcoming European elections? What does this mean for Russia's role and sanctions? What will occur with US banking regulations and how will that impact us? Over 100 days on and we have more insight into these questions, but still plenty of uncertainty and unpredictability.

Not surprisingly, over one-third (37%) of large UK retail / wholesale banks selected geo-political events as the single biggest risk to their organisation during the coming year. That's nearly as many (42%) who selected evolving criminal methods.

6.1 So what happens now?

"With Trump, there's uncertainty..."

Changes in current sanctions agreements, with respect to Iran and Russia, are a key concern among UK banks; not knowing what the landscape will look like in two years can impact investment appetite today.

As mentioned by one of our interviewees, "I think Iran and Russia will be of concern. Particularly Iran. Most people don't want to do Iranian business because nobody wants to do anything long-term and then discover that something gets in the way in just two years' time."

There is uncertainty as to whether the US administration may reverse American policy on the 2015 international agreement aimed at curbing Iran's nuclear program and easing sanctions. Whilst the waiver of 17th May, 2017 avoided any US sanction 'snapback' relating to the 2015 nuclear agreement, further sanctions on Iranian defence officials, relating to the development of ballistic missiles, were announced in the same media note.

The UK Prime Minister and other European leaders have publically supported the agreement, and a move by the White House to reinstate some or all of the sanctions would certainly throw business deals into a quandary. A disparate western position could lead to increased cost and complexity of implementation.

We must also consider the US administration's relationship with Russia. Questions abound as to whether sanctions against Russia will continue or be eased. Recent months have seen the concerns around this abate somewhat as events in Syria have seen Washington/Moscow relations cool further. However, in the current highly unpredictable political climate that position could change in a moment.

> "With Trump, there's uncertainty! Who knows where he's going to go on Russia and Iran. Will sanctions tools be something they use and, if so, how and against whom?"

Uncertainty also extends to whatever actions the Trump administration pursues with current regulatory policy. The president has been public about his dislike of regulation which stifles big business, including US banking competition and profitability; such as the Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).

In early February 2017, President Trump signed an Executive Order that directed the Treasury Secretary to review which Dodd-Frank regulations could be changed or repealed.[50] The Republican-controlled members of the US Congress also passed legislation scrapping anti-corruption measures from Dodd-Frank eliminating transparency requirements for US oil and mining company payments to foreign governments.[51] More changes are likely to come, as President Trump has commented that "we expect to be cutting a lot out of Dodd-Frank".[52]

Whilst various facets of Dodd-Frank were intended to regulate US banking behaviour and protect consumers, the repeal of the payments transparency for extraction companies' could impact financial crime compliance for multinational banks in the UK. Specifically, this adds blind spots into payment transactions which could potentially go through banks located within the UK.

Past experience suggests this is a significant concern, according to Jodi Vittori, an adjunct professor teaching terrorism finance at Georgetown University, Washington D.C., who has also worked with NATO counter-corruption efforts. A lot of the money paid by the gas and oil industry to poor or fragile countries "gets diverted to other places," she warned – "to hackers... terrorists, insurgents, warlords [and] criminals".[53]

The end result may look very different. Many financial regulations are written and enforced by non-governmental organisations dedicated to regulation itself. This includes the Financial Industry Regulation Authority (FINRA), which has signalled that it foresees no significant regulatory changes in 2017, including those related to money laundering.[54] And, of course, any sizeable overhaul of Dodd-Frank would need to pass Congress. Lastly, the US Treasury's power is not unlimited; it doesn't directly supervise banks or control the actions of bureaus such as the Financial Crimes Enforcement Network (FINCEN) which oversees anti-money laundering rules.[55]

Some US banks have expressed the belief that the Trump Administration will remain tough on AML compliance. The former head of the US Office of the Comptroller of the Currency and now chief executive of Promontory Financial Group, Gene Ludwig, believes that tougher anti-terror comments and stances by the new administration signal money laundering as a continued "serious area of focus".[56]

50. http://thehill.com/policy/finance/317799-trump-signs-executive-orders-to-loosen-wall-street-regs
51. http://www.usatoday.com/story/money/2017/02/14/trump-scraps-dodd-frank-rule-resource-extraction-disclosure/97912600/
52. http://www.lexology.com/library/detail.aspx?g=0462f133-4967-4628-9eb3-9c244732fdc0
53. http://edition.cnn.com/2017/01/31/politics/oil-industry-regulations/
54. http://www.lexology.com/library/detail.aspx?g=ada36042-6dea-48e9-b14e-63e8969c875d
55. http://www.lexology.com/library/detail.aspx?g=0462f133-4967-4628-9eb3-9c244732fdc0
56. https://www.ft.com/content/fdf88c84-e89a-11e6-893c-082c54a7f539

6.2 Brexit

"Let's get on with it..."

During early research interviews, there was mention among some that Brexit would have less impact than may be expected on the UK financial sector in terms of financial crime legislation. There was an expectation of the adoption of current EU laws which the UK was involved in creating in the first place. As one interviewee put it, *"I think from a financial crimes perspective, the laws that we've got in place – I mean, the whole of the ethos of much of the EU legislation is shaped by British thinking, anyway. And so the fact that we're coming out of it, I don't think our laws are going to fundamentally change. We might tweak a little bit here and there."*

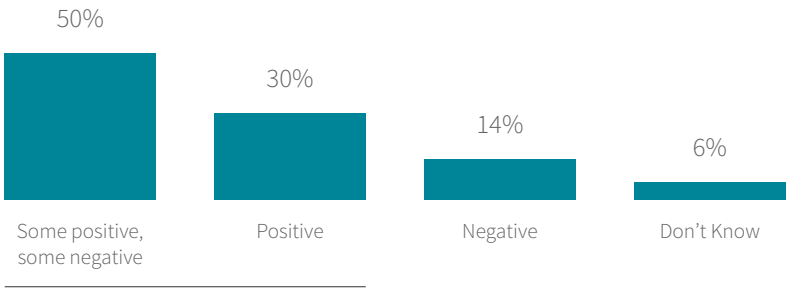
The question is whether the UK will continue to update laws as the EU inevitably does so with its regulations, when it may not have a seat or a significant say in the drafting and evolution of such legislation.

Results from our survey among a larger audience of financial crime professionals showed a cautious optimism about the UK's ability to combat financial crime following Brexit.

Figure 28

Q: Do you believe that Brexit will have a positive or negative impact on the UK's ability to combat financial crime? (n = 168)

Positive or negative impact of Brexit on the UK's ability to combat financial crime



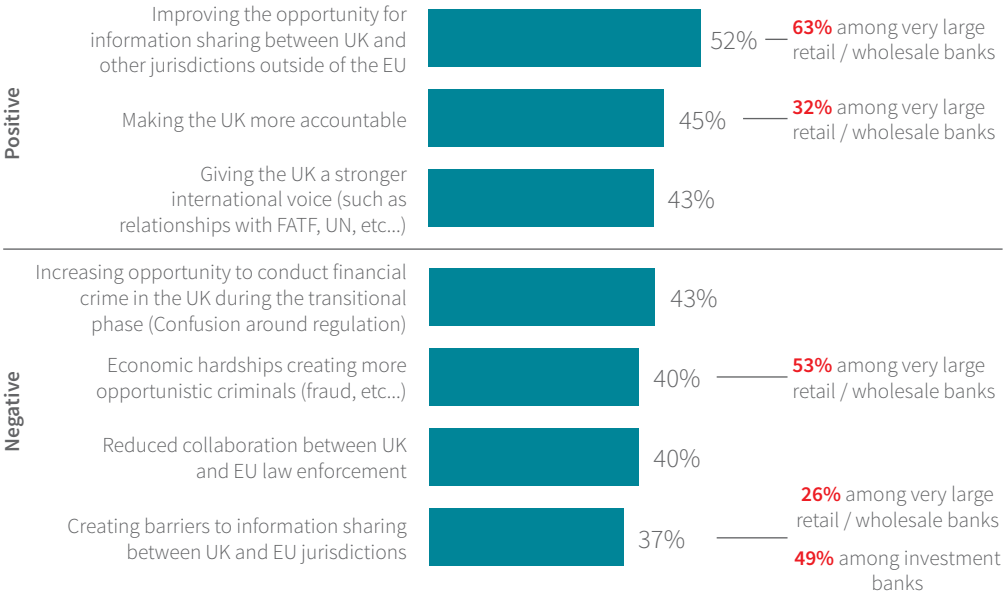
80% Positive to some degree

Half or more survey respondents expect that Brexit will help provide opportunities to improve information sharing between the UK and other non-EU jurisdictions. Nearly half felt that Brexit will make the UK more accountable and give it a stronger international voice in terms of financial crime fighting but it was early days. There was, however, a sizeable minority who also expect some negative impacts such as creating more crime, reducing information sharing between UK and EU jurisdictions and generating more friction between the UK and EU authorities.

Figure 29

Q: Which of the following do you expect to be the Top 3 impacts from Brexit? (Respondents could select more than one option; n = 168)

Top 3 expected impacts from Brexit?



Of course the ability to share information within and between banks both in the UK and across EU borders will depend in no large part upon any adequacy agreement reached between the UK and the EU for the purposes of data transfer. This will be a key issue for the financial sector in both the UK and in other EU countries. Indeed, given the importance of data transfers across borders to a wide range of industries, including tech, energy and the automotive industry, it is clear this will be a critical area for the UK and the EU to focus upon, and yet it is not an issue that currently has widespread focus.

Elsewhere on Brexit, respondents from larger retail / wholesale banks expressed mixed expectations. In addition to strongly expecting better information sharing, they are less confident that Brexit would make the UK more accountable.

Also, more than half (53%) of large retail / wholesale survey respondents said they believe Brexit could generate more criminals where it creates economic hardships.

But whilst Brexit negotiations and full separation are a way off, the fight against financial crime in the UK will still draw on EU derived legislation, with the EU's Fourth Anti-Money Laundering (AML) Directive being transposed into domestic law by mid-year as the drafting of the Fifth Directive continues to evolve. Of course, in the future this position could change, but any divergence in policy and legislation by the UK from the EU will likely lead to increased costs and complexities of implementation for organisations.

That said, the UK remains at the vanguard of the charge, having heavily influenced the Fourth AML Directive, driving the requirement for all EU member states to establish Company Beneficial Ownership registers. There is little doubt that the UK will remain a prominent player in the fight against financial crime, continuing its membership of the Financial Action Task Force.[57]

Brexit should not impact the UK's sanctions positions. Many of these are UN mandated, which isn't affected by leaving the EU and whilst the UK may seek to strengthen some of its sanctions laws, it will need to keep in mind the ability for these to work within the parameters set by other global partners, including the EU.[58] The flip side is if the UK seeks to lessen sanctions restrictions from current EU positions; that could have a negative impact of increasing financial crime in the UK as a way of circumventing EU sanctions.[59]

Whilst Brexit may provide opportunities for the professional criminal or create unwitting fraudsters, it is believed unlikely to cause a dramatic rise in financial crime issues in the UK.

2017 is proving to be a year of transition, indeed it is creating political drama of its own. This of course adds uncertainties. For now, though, it appears that neither Brexit nor the new American administration will significantly upset the industrialised effort to fight financial crime.

Instead, we should probably expect the UK, and its banking industry, to continue to play a leading role in the fight against financial crime in the future – whatever changes arise.

57. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564813/impact_assessment_transposition_of_4MLD.pdf
58. http://www.elexica.com/en/legal-topics/crime-fraud-and-investigations/18-the-implications-for-financial-crime-and-investigations
59. Ibid

Observations of LexisNexis® Risk Solutions

A sharp eye on the US

The repeal of the US Cardin-Lugar anti-corruption rules from Dodd-Frank could create additional challenges for UK banks. Business relationships with US based or listed oil, gas and mineral extraction businesses (and transactions on their behalf), will have to be carefully scrutinised to ensure compliance and demonstrate financial transparency.

In addition to regulation, another topic high on the agenda for the new administration is the Security of the United States and the effective past use of sectoral sanctions could provide an alternative to military action. Whilst more effective for government and society, the cost for financial services companies increases in this more complex geo-political regime. Also, the divergence of sanctions regimes between the US and EU on issues such as Russia and Iran makes business decisions and implementation much harder.

A parting of ways

Whilst sentiment during our interviews led toward the UK retaining EU legislation, there is a real possibility of subsequent divergence if the UK does not maintain a prominent seat in the drafting of such future legislation. This could result in the UK losing its 'equivalent' status and lead to two differing financial crime compliance standards between the UK and EU that financial institutions would have to manage. In turn this would not only create more cost for banks (in terms of implementation, management and lost custom), but could potentially provide opportunities for criminals to exploit, as they look for gaps between regimes.

7. Methodology

LexisNexis® Risk Solutions conducted research between November 2016 and February 2017 with banks in the UK and law enforcement. KS&R Inc., a global market research firm, was contracted to manage these efforts which included three components:

- In-person interviews with senior level financial crime / AML compliance and law enforcement professionals;
- 168 online surveys with the above types of banking professionals; and
- Secondary research of issues, trends and related topics around financial crime and geo-political events.

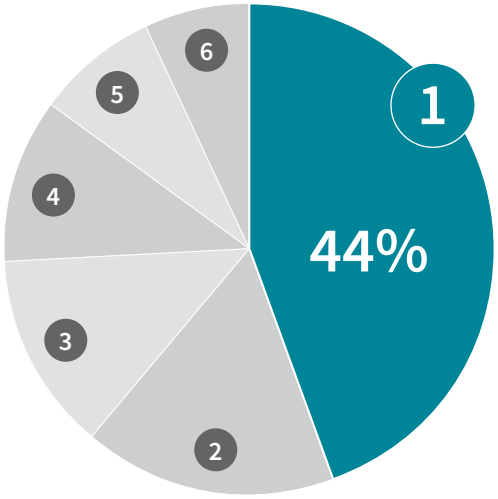
Extensive analysis and resource time has been expended to ensure that findings are both rigorous and objective.

During the research, LexisNexis® Risk Solutions was identified as the sponsor.

8. Appendix

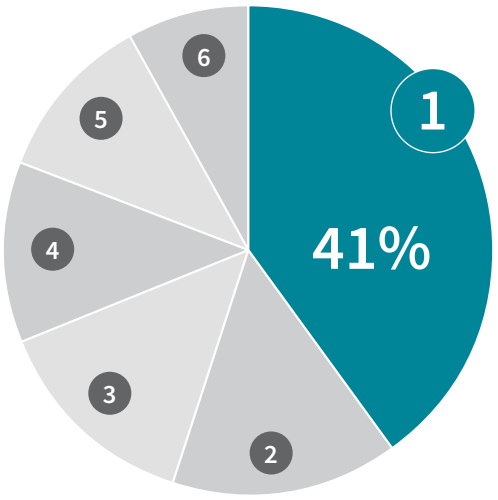
The following diagrams highlight the results of the online survey of senior financial crime compliance professionals working for banks in the UK. Conducted between January and February in 2017, the survey secured 168 responses

Q: What would you say is the biggest single financial crime risk to your business at the present time? (n = 168)



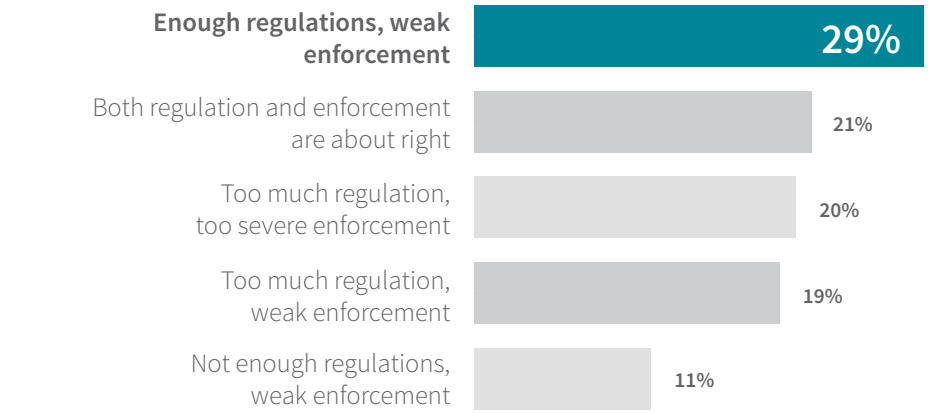
1. **Evolving criminal methodologies (e.g., cybercrime, etc…)**
2. Cost of AML compliance - **17%**
3. Geo-political events - **13%**
4. Lack of personnel in your risk function - **11%**
5. Civil prosecutions/class actions - **8%**
6. Sanctions - **7%**

Q: What do you think will be the biggest single emerging financial crime risk to your business in the next 12 months? (n = 168)

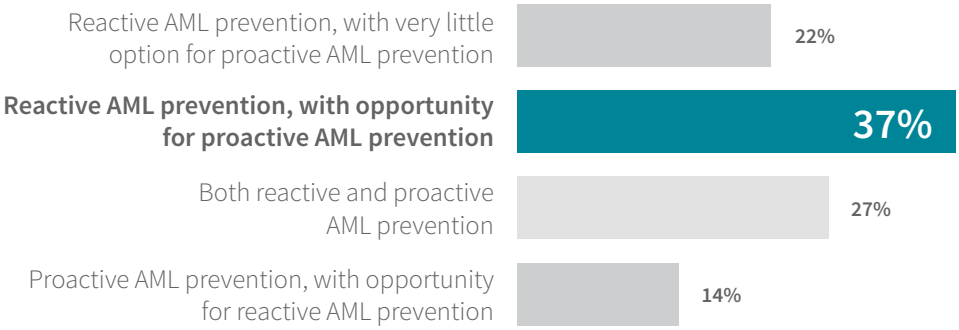


1. **Evolving criminal methodologies (e.g., cybercrime, etc…)**
2. Geo-political events - **15%**
3. Cost of AML compliance - **14%**
4. Lack of personnel in your risk function - **12%**
5. Civil prosecutions/class actions - **11%**
6. Sanctions - **7%**

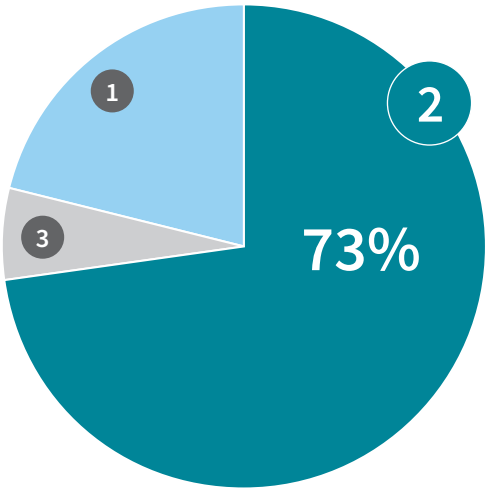
Q: How would you describe the current overall levels of UK financial crime regulations and enforcement in the UK banking sector? (n = 168)



Q: Which of the following statements do you most agree with? Would you say that the current UK financial crime risk compliance structure is focused on... (n = 168)



Q: Will the introduction of the 4th EU AML Directive make it more or less difficult for banks to effectively prevent money laundering? (n = 168)

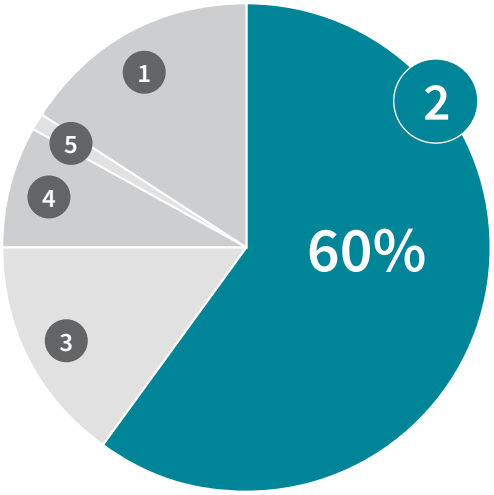


1 Will not make it any more or less difficult than it is now **21%**

Make it less difficult

3 Make it more difficult - **6%**

Q: When implemented, what impact do you think the AML Action Plan & Criminal Finances Bill* will have on levels of money laundering in the UK? (n = 168)



1 Drastically reduce levels of money laundering - **16%**

Will reduce money laundering levels somewhat

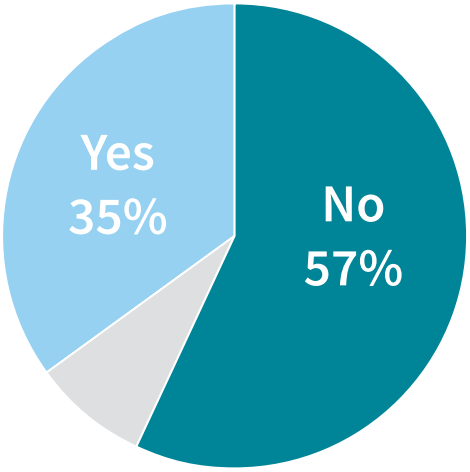
3 Will make no difference - **15%**

4 Will increase money laundering levels somewhat - **8%**

5 Drastically increase levels of money laundering - **1%**

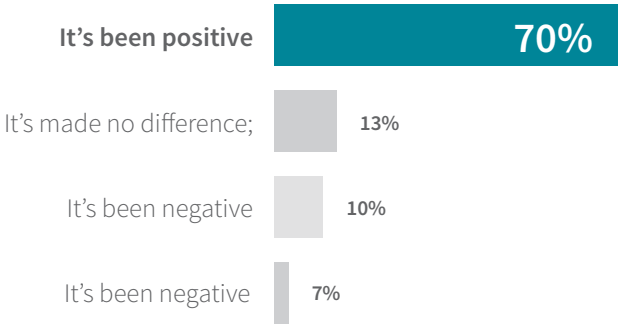
* The interviews and online surveys which generated this report were conducted prior to the Criminal Finances Bill becoming the Criminal Finances Act 2017 on April 27th 2017.

Q: If you had the opportunity, would you choose a career path other than financial crime compliance, in light of the increased regulatory pressures? (n = 168)

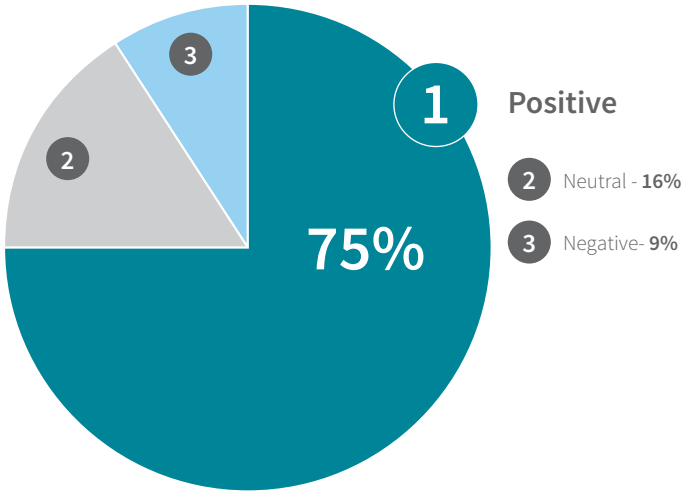


Don't know - **8%**

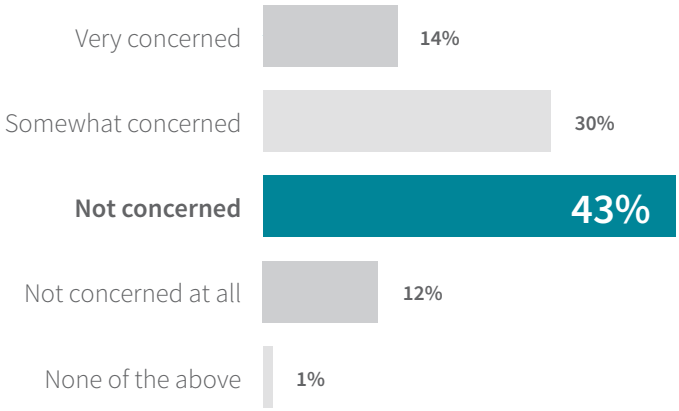
Q Overall, has the policy of making executives personally responsible for the actions of employees within their firms been positive or negative for the industry? (n = 168)



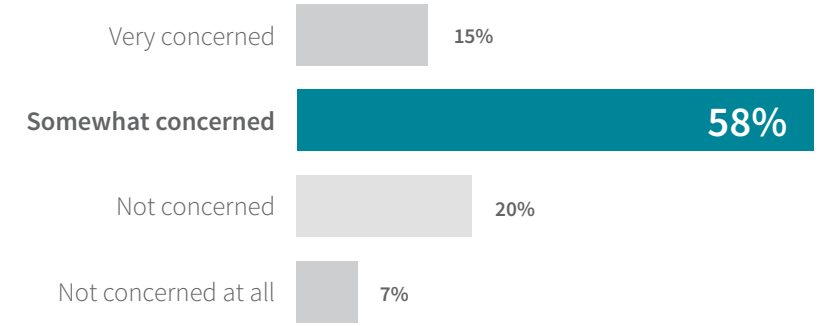
Q: How would you rate the impact of the Senior Managers Regime (SMR) on your organisation's risk appetite? (n = 168)



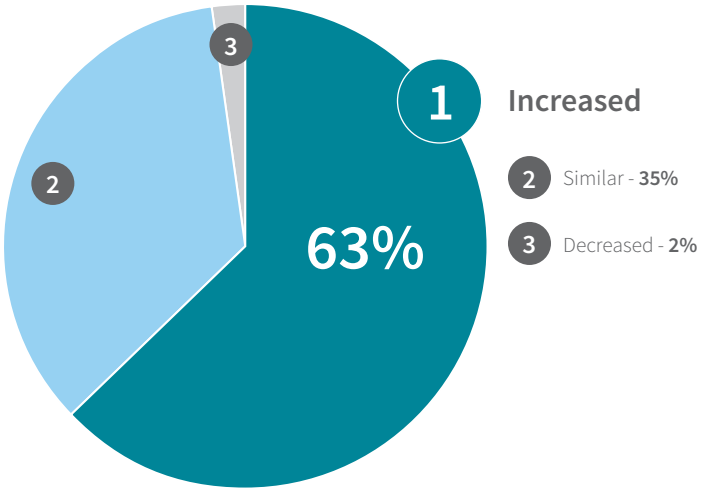
Q: How concerned are you about the impact of tax evasion on your business in the next 1-2 years? (n = 168)



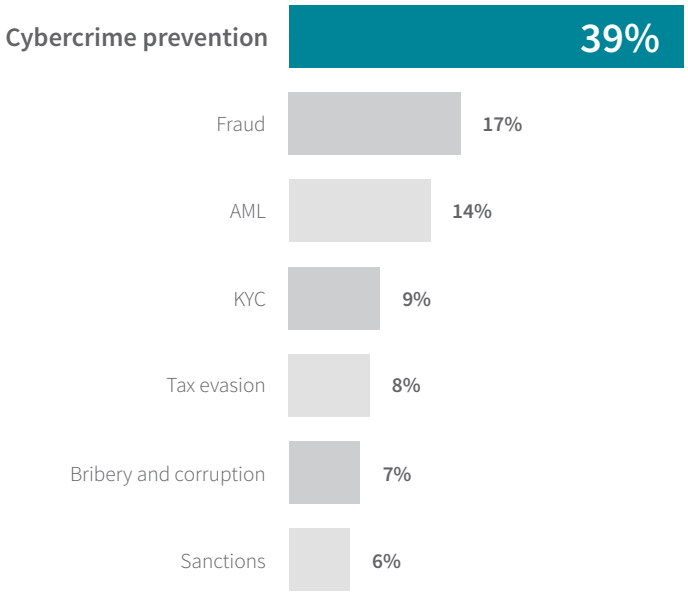
Q: How concerned are you about the impact of corruption on your business in the next 1-2 years? (n = 168)



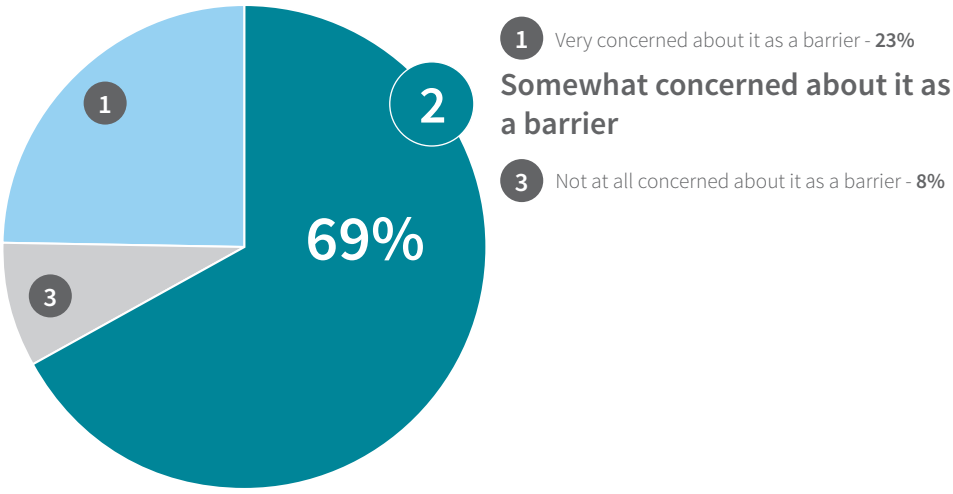
Q: What has been the trend with the cost of compliance in your organisation over the past 2 years? (n = 168)



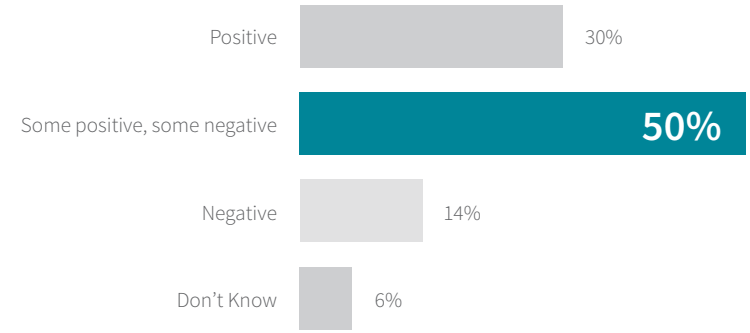
Q: Where do you think the greatest single area of investment in financial crime prevention will happen in your business over the next 1-2 years? (n = 168)



Q: How concerned is your organisation about the impact of legacy technology as a barrier to fighting financial crime during the next 1–2 years? (n = 168)



Q: Do you believe that Brexit will have a positive or negative impact on the UK's ability to combat financial crime? (n = 168)



Q: Which of the following do you expect to be the Top 3 impacts from Brexit? (Respondents could select more than one option; n = 168)

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

lexisnexis.com/risk/tracesmart

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

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

About KS&R, Inc.

KS&R is a multi-award winning supplier of global market research. The firm works closely with clients in a range of industries to improve market position and increase returns on marketing investments.