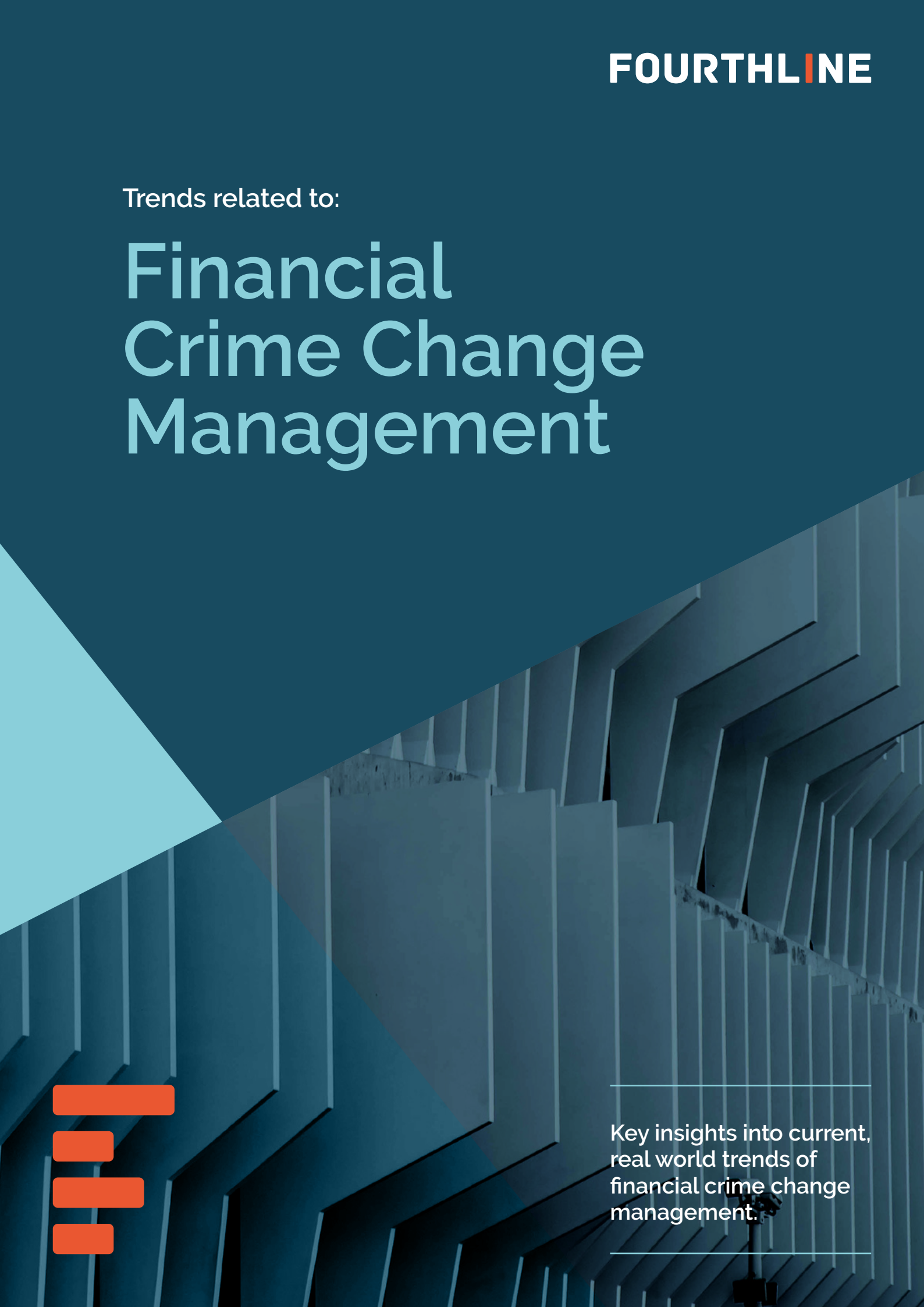
FOURTHLINE

Trends related to:

Financial Crime Change Management



Key insights into current, real world trends of financial crime change management.

We interviewed five well-respected financial crime professionals to understand the current, real-world trends of financial crime change management, barriers, and solutions aimed at stemming criminal activity. As a result, we have been able to provide key insights into the current state of financial crime and how firms can use expertise to implement successful crime prevention through change management.

Key takeaways:

* A firm's willingness to understand risk, the leadership tone, shared knowledge, and a model of continuous self-improvement are of equal importance to technological advancement.
* A drive to see a more holistic view of financial crime has led to a gradual departure from siloed information.
* There is nervousness from professionals around less-regulated counterparts in the industry.
* The Government's Economic Crime Plan 2019-22, The Fifth Money Laundering Directive, and Brexit-related legislation are all critical regulatory developments.
* FinTechs are finally starting to employ tenured, ex-banking financial crime professionals to adequately prevent and manage risk – a chink in the chain of financial crime.
* The training and performance management of the team is essential to reducing financial crime within a firm.
* A robust monitoring and reporting regime, which is supported by powerful technology, is vital.
* Working together, keeping abreast of regulatory changes, and ensuring that there are appropriate change governance processes must be at the heart of the business model.

Executive Summary

It's clear that firms are more technologically equipped to tackle financial crime than ever before, but is that enough? As far as the financial crime professionals we interviewed are concerned, advancements in software are simply the power behind what must be an experienced, well-trained team to harness any insights.

A firm's willingness to prioritise financial crime change management, set the tone at the top, and develop their team is vital to identifying, investigating, and reporting activity. Moreover, it's a firm's commitment to self-improvement strategies and the sharing of knowledge across Governing bodies and regulators that will arm firms with the power to prevent and manage financial crime.

Acknowledgement that criminals don't rest, and amidst nervousness that new entrants in the market are ripe for financial crime, sees the introduction of the Government's Economic Crime Plan 2019-22 and the Fifth Money Laundering Directive.

All of the financial crime professionals seem to concur on one fact: we need to ditch silos and work together, both in terms of people and data insight to gain a holistic view of criminal activity.

HM's Government and the Financial Conduct Authority (FCA) jointly acknowledge that financial crime can only be combated by harnessing the capabilities, resources, and experience of both the public and private sectors.

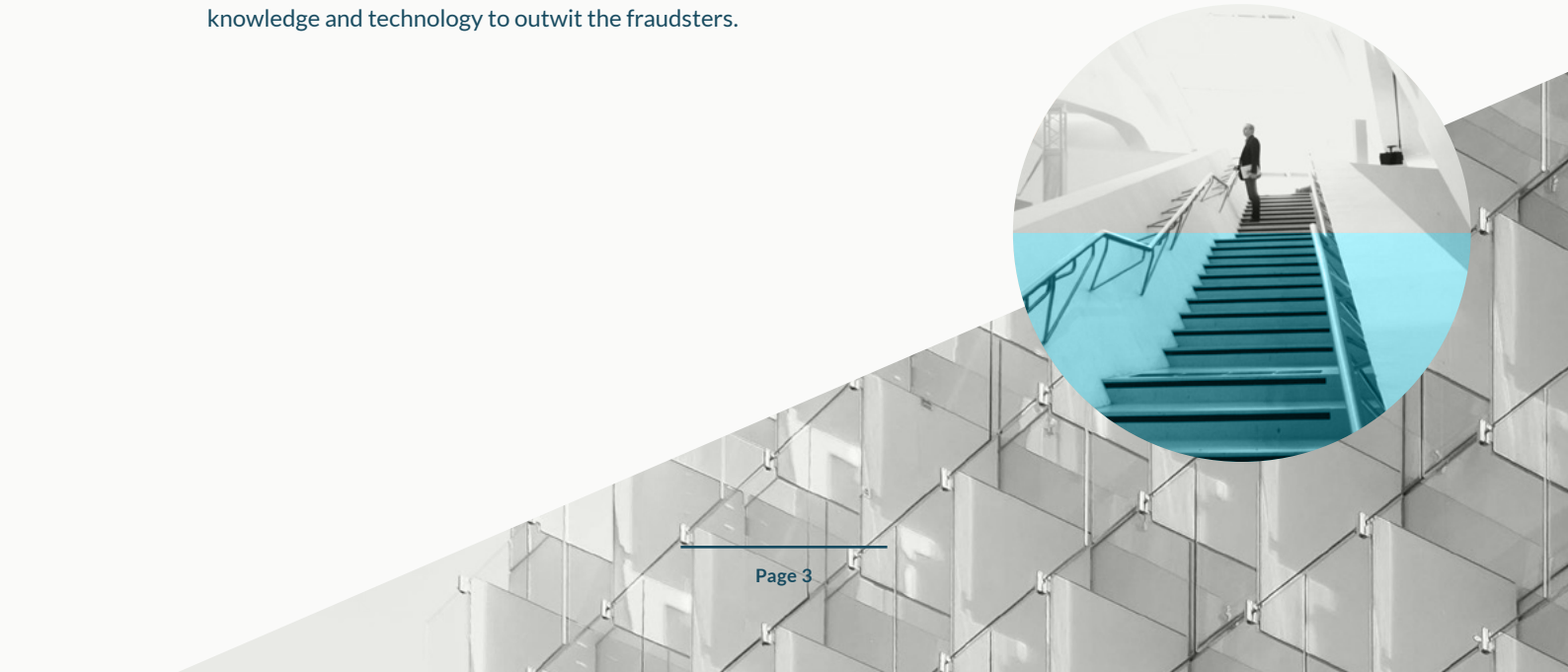
HM's Government is focussed on the threat to the security and prosperity of the UK as it impacts everyone in society, including citizens, private sector businesses, and the Government. However, as one in 15 people fall victim to fraud, the responsibility to protect the general public and mitigate financial loss continues to sit heavily on the shoulders of private firms.

The ever-evolving, clandestine nature of financial crime, and increased capacity to obscure sources, as highlighted by the Government and financial crime professionals, lends itself to a new, evolving strategy — financial crime change management.

It has never been more important for business leaders and senior financial crime professionals to set the tone and develop business-wide, self-improvement strategies on financial crime, according to the FCA, at a time when:

* The UK exits the EU
* Digital transformation takes hold
* The propensity of new market entrants is high
* There is an increased opportunity to obscure financial source
* The Government's Economic Crime plan 2019-22 sets out targets

Private firms have the opportunity to employ the services of technically minded and experienced financial crime professionals to harness the power of shared knowledge and technology to outwit the fraudsters.



The FCA places emphasis on technology, data, and agency engagement.

In the latest publication, the FCA continues to prioritise combatting financial crime and improving anti-money laundering practices, stating that the use of technology, data, and engaging with Government bodies and agencies as the key to success.

Clear leadership and development of a strategy to address financial crime change management are vital for helping an organisation to respond to an evolving challenge. In creating this culture of continuous self-improvement internally, the firm will also protect the consumers they serve. Criminals don't stand still, so neither can an organisation.

The insights gained from our research with five well-respected financial crime change management professionals are somewhat also reflected in the FCA's view of a poor versus a good practice approach to managing financial crime.

Good practice

* Senior management set the right tone and demonstrate leadership on financial crime issues.
* A firm takes active steps to prevent criminals from taking advantage of its services.
* A firm has a strategy for self-improvement on financial crime.
* There are clear criteria for escalating financial crime issues.

Poor practice

* There is little evidence of senior staff involvement and challenge in practice.
* A firm concentrates on narrow compliance with minimum regulatory standards and has little engagement with issues.
* Financial crime issues are dealt with on a purely reactive basis.
* There is no meaningful record or evidence of senior management considering financial crime risks.

The state of financial crime and fraud management readiness within firms

The consensus from financial crime professionals interviewed is that firms have never been as technically equipped to identify, investigate, and report criminal acts. However, the professionals have also recognised that a firm's willingness to understand risk, the leadership tone, shared knowledge, and a model of continuous self-improvement are of equal importance.

What are the views of the Financial Crime professionals?

> A firm's readiness really depends on the organisation's willingness to understand the risks the business faces and the tone from the top.
>
> Toby Serkovich

Firms need to have accurate and up to date financial crime risk assessments that consider all the financial crime disciplines.

The risk assessment process needs to be ever-evolving, identifying, and then mitigating areas of concern as they emerge.

A firm's readiness varies from poor to acceptable due to lack of will, incomplete knowledge or understanding of various risks, and poor or non-existent risk assessments.

The firm's leadership focus, culture, and attitude are key drivers of financial crime awareness.

Banks should now be in a good position to detect and reduce levels of financial crime risk. However, there always remains further work to do given the constantly changing nature of the regulatory and wider financial crime landscape.

I think the FinTech community's resilience to financial crime can be viewed in two, polarised ways. On the one hand, we have never been better equipped in terms of the technology available to us to identify, investigate, and report criminal actors or unusual transactions. However, the more competition there is in the payments and financial services market, the more fragmented the flows become, producing a ripe proving ground to criminals for obscuring the source, transit, and ultimate destination of illicit funds.

Unless we really start talking about what we are seeing as individual institutions and piece that together, we are still at the mercy of criminals who seek to exploit the fast-paced, customer-centric business model that we are all competing for within the industry.

Charlie Greer

What are the developments taking place across the market that influence how firms manage financial crime?

A drive to see a more holistic view of financial crime has led to a gradual departure from siloed information; this is resulting in a wider picture of criminal activity. There is, however, a nervousness from professionals around less-regulated counterparts in the industry.

What are the views of the Financial Crime professionals?

There is a wider drive to see a consolidated view – financial crime is no longer siloed, but firms are developing teams that are able to see the whole view on financial crime within the firm.

FinTechs still need the support of clearing banks to service their customers. These banks do not enjoy the same latitude as their less regulated counterparts.

What we are noting is an increase in major systemic failures in AML and related activities. It is likely that we will see more acute individual liability for personnel in the AML and related governance process.

The key here is probably regulatory visits; with the FCA having visited most larger firms and continuing to focus on small firms in more recent years.

The move to online and mobile services including cryptocurrencies provides additional challenges to firms to try and keep pace with development.

> Overall, I see the banks filling the gaps left by regulators, whether intentionally or not, with increasingly tough expectations. They will implement strict risk appetites that FinTech's must abide by, and those who don't will be left to find other providers in a rapidly diminishing pool. Those who are able to keep up because they possess the right combination of risk, talent, expertise, and technology will be the ones that survive.
>
> **Charlie Greer**

When looking into the horizon, what market and regulatory developments are likely to impact how firms manage financial crime?

The Financial Crime professionals identified that the Government's Economic Crime Plan 2019-22, The Fifth Money Laundering Directive, and Brexit-related legislation are all key regulatory developments in terms of a firm's ability to manage financial crime effectively.

What are the views of the Financial Crime professionals?

While the Government has enacted instruments to ensure legislation will be in place post-Brexit, firms will need to revisit their risk appetites to consider if their business model is fit for purpose.

HM Treasury has recently sought views on regulatory coordination in the financial service sector to determine the long-term effectiveness of the regulatory regime, which will also examine how the framework should adapt post-Brexit once details of the future relationship are clear.

There will always be the minimum standards required of institutions within the financial services environment governing financial crime risk management. The differentiator will be the application of these regulations on an institution-by-institution basis.

The regulatory backlash to high-profile failures still needs to be seen. I expect an increasing number of investigations -- a key factor is reducing the time of investigating and charging corporations and individuals.

> SMCR, GDPR, PSD II, Law Commission Review, and Brexit related changes are all regulatory developments that will play a part in a firm's ability to manage financial crime.
>
> **Ian Stevenson**

> The Economic Crime plan 2019-22 presents food for thought around the Government's actions in seven key areas regarding Financial Crime. This report also feeds into the findings of the FATF mutual evaluation of the UK at the end of the year and includes an overhaul of the SARs regime, reviewing the criminal market abuse regime, increasing public and private sector collaboration, amending the Proceeds of Crime Act, considering a new power to block company listings on UK-regulated markets on national security grounds, and reviewing the criminal market abuse regime. The Fifth Money Laundering Directive is another important element, which was also included in the Government's Economic Crime plan as legislation they needed to implement.

Toby Serkovich

How would you analyse the main contributing factors to a firm's weaknesses and failures of financial crime systems and controls?

Financial professionals believe that weaknesses and failures are best understood by analysing recent cases of fines from the FCA. Recently, this has identified the importance of due diligence, shared information, experience, and internal communication. There is also a feeling that FinTech companies are finally starting to employ tenured, ex-banking financial crime professionals – a weakness among new market entrants.

What are the views of the Financial Crime professionals?

Despite clear improvements in the quality of talent available within the market, there are still natural tensions between experience and cost. Good people cost money, and FinTechs are often reluctant to invest too heavily in experienced people upfront while they are in a start-up stage. Fortunately, it feels like the tide is beginning to turn, with firms starting to actively pursue more tenured talent.

Shockingly poor risk assessments, lack of enforcement action, non-existence or oversight from audit/risk committees, poor knowledge, and insufficient training remain key weaknesses within firms across the UK.

Poor leadership focus and accountability that drives minimalist and token 'process' compliance remain an issue for firms.

Lack of benchmark with other firms either directly or via industry forums such as UK Finance MLAP or MLRO Network.

> "Primarily, failure to keep up with regulation, lack of acknowledgement by senior management of their obligations and providing 'tone from the top', resulting in inadequate investment or poor-risk acceptance. A lack of experience in staff and failure to upskill and appropriately horizon scan for change"
>
> Tim Stewart

> The ability of firms to know who the clients are and to ensure they are appropriately risk-rated resonates again in the fine for **Deutsche Bank for £163 million in 2017**. The firm performed inadequate customer due diligence, used flawed risk rating methodology, deficient AML policies and procedures, and lacked appropriate systems for detecting suspicious transactions. There was confusion as to who was tasked with client due diligence – one team thought another team had conducted this and vice versa."
>
> **Toby Serkovich**

How can firms improve their people, process, and technology systems to better manage, and reduce financial crime related risks?

The training and performance management of the team is essential to reducing financial crime within a firm. A person's knowledge is a key asset, so joining up what's in a head and a computer is vital. The business model and tone from the top must be one of continuous improvement and common sense. A robust monitoring and reporting regime, which is supported by powerful technology is essential, according to professionals interviewed.

What are the views of the Financial Crime professionals?

By ensuring their staff are suitably trained, risks are identified, and an evolving risk assessment and framework which is in line with the business and the threats identified is in place.

Firms need a transaction monitoring regime in place which reflects a firm's risk appetite and is considered regularly to ensure it is still suitable and functioning as expected.

Leadership at all levels must be more individually and financially accountable. Proper and robust external reviews and challenges should be encouraged. Make all people in a division accountable for process failures (with bonus and KPI impacts).

A strong whistleblowing culture and lucrative reward system must be encouraged.

Training is vital, ensuring staff are provided with a holistic understanding of financial crime risk management so that they understand how the key elements of the financial crime risk management framework fit together. This will help avoid working in silos.

> Understanding and documenting their business model(s) and sources of FC risk, make it simple, use common sense, take holistic views to totality of control environment. Don't forget all that information in people's heads and in other places, benchmark vs. your sector/risk profile, make everything customer-friendly, and use technology delivered through APIs/online – which require less IT involvement and provide greater flexibility.
>
> **Ian Stevenson**

What technological innovations do you expect to take place across the market to help firms detect, control, and reduce financial crime related risks?

Financial crime professionals perceive screening and identifying suspicious transactions as essential to every firm in preventing financial crime. This identification is becoming easier with FinTech, AI, open-source software, and cloud-based solutions. Simplistic algorithms do not take advantage, or have the processing power, to analyse the data available and shared knowledge needed to create red flags on suspicious activity.

What are the views of the Financial Crime professionals?

There is considerable discussion, certainly from the regulator around Fintech, and how it can be used to identify potentially suspicious transactions as part of an efficient transaction monitoring regime.

Fintechs, AI, more open-source software, greater use of 'registry' type services, and increased use of cloud-based solutions will help detect, control, and reduce financial crime.

There needs to be an improvement in the data collection process and the pro-active analysis of the data. The primary challenges are managing:

* Disparate source systems (credit agencies, PEP Lists, company ownership registers)
* Outdated and redundant data (clutter)
* Gaps in key data elements
* Meaningful analysis of alerts and trends
* Prompt and pro-active action on the alerts.

> I see more use of the visualisation tools (PowerBI, Qlikview, etc), in the hands of specialists, combined with increasing use of AI to analyse the data for hidden trends. Simplistic algorithms can only do so much
>
> **Tim Stewart**

More network-based systems that can track transactions through multiple customers and other banks. Continuation of a move to 'online' customer verification.

Expansion into machine discounting of alerts based on algorithms rather than manual review.

What advice would you give to firms looking to improve financial crime change management?

Working together, keeping abreast of regulatory changes continuously, and ensuring that there are appropriate change governance processes must be at the heart of the business model, according to the financial crime professionals. There must be an appreciation that both people and technology are equally important in the battle against financial crime.

What is the advice from the financial crime professionals?

1. Sign up to trusted regulatory news providers, engage with industry bodies and like-minded working parties, and ensure feedback is provided on consultation papers to inform future legislation and shared learning.

2. Track legislation and ensure appropriate change governance processes are in place within the firm when it comes to implementation.

3. Implement individual accountability, clear business processes, and sufficient resources – both systems and people-based, both quantum and quality, flexible systems, and sensible risk appetite setting and metrics.

4. Place emphasis on sustained continuous improvement, which must be enforced from the top down. The clear understanding of the AML objectives, data points, and the processing of said information must be properly understood by key leadership.

5. Prioritise activities rather than try and complete them all at once. Especially consider the hierarchy, for example, agree risk assessment, risk appetite, policy, and standards first, before rolling out new processes or starting remediating customers.

6. Carefully consider tech solution providers, as they can often promise the earth, but may not work for more bespoke firms with niche customers or will often only cover part of the customer population. Try and keep BAU engagement as much as possible, to ensure that the business is set up and engaged to receive change.

Acknowledgements

FourthLine would like to thank the following financial crime professionals for providing their insights towards this whitepaper.

Charlie Greer

Head of Financial Crime at WorldFirst

Toby Serkovich

Deputy Money Laundering Reporting Officer at Old Mutual Wealth Ltd and Old Mutual Wealth Life and Pensions Ltd

Ian Stevenson

Managing Consultant at Strategic Regulatory Management Limited

Tim Stewart

Head of Compliance at Committed Capital Financial Services Ltd

Plus a further contributor who wished to remain anonymous.

We would also like to thank the following FourthLine internal experts for their contributions:

David Croft

Jakes De Kock

Thom Docking

Tom Littlewood

FOURTHLINE

About FourthLine Consulting

FourthLine is a risk management consultancy that offers talent, learning and consultancy solutions. We combine expert insight, an enviable client list and a network of extraordinary talent to help our clients make critical hires that prevent risk in their operations, whilst our micro-learning solutions help improve individual and team performance throughout the year.

Our highly trained consultants have an unrivalled up-to-date understanding of their specialist fields and our interim, talent and retained resourcing solutions are used by more businesses than ever before.

If you are looking to improve your financial crime change management by bringing in a partner to support with your talent and learning requirements, our Financial Crime team can help.

Contact:
Tom Littlewood
Senior Consultant – Financial Crime

tom.littlewood@thefourthline.co.uk
0203 762 2436

Tom joined FourthLine in January 2019, bringing over 9 years of interim recruitment experience having had success across other sectors.

As a Senior Consultant at FourthLine, Tom's area of specialism is across Financial Crime & Compliance within Financial Services.

Visit our website
www.thefourthline.co.uk
for more information about the range of services we offer or give us a call on
0203 800 1099.