FINANCIAL REGULATION EMERGING THEMES IN 2020

10 YEARS OF EMERGING THEMES IN FINANCIAL REGULATION

10 YEARS 2020

GLOBAL REGULATION

LOCAL SOLUTIONS

FEATURED CONTENT

BRYAN CAVE LEIGHTON PAISNER

GLOBAL REGULATION, LOCAL SOLUTIONS.

Welcome to the 2020 edition of Emerging Themes, our annual collection of personal reflections on new and emerging issues in financial regulation.

Welcome to the 2020 edition of our *Emerging Themes in Financial Regulation* publication, a collection of personal viewpoints and insights from members of our global team on new developments in the regulatory landscape that will help you manage your legal and compliance risks in the year ahead and beyond.

We are celebrating our 10th anniversary publication, and in that time since 2010 we have predicted and charted huge change across the regulatory landscape. As even a quick look at the articles will indicate, the environment continues to evolve at a rapid pace.

Our overarching theme this year is *"Global Regulation, Local Solutions"*. More than ever, misconduct can lead to consequences with multiple agencies spanning a range of jurisdictions as well as a range of related authorities – not just financial regulators, but criminal authorities, data protection agencies, antitrust authorities, and bodies responsible for equal opportunities. This is on top of the risk of civil claims being pursued. Having global capabilities to manage legal and regulatory risks in each of the main jurisdictions is key, but equally important is recognising the unique approaches and expectations of each relevant authority. Having a genuine depth of understanding of the local regime, the priorities of the regulator and its decision-making processes will be critical in developing a tailored strategy and achieving the best available outcome for the group.

One pervasive factor that has perhaps led to the greatest change in this last decade is the huge impact of technology and data on the management of regulatory risk – as highlighted in our 2018 edition of *Emerging Themes, "Regulation in the Information Age"*.[1] This impacts financial institutions at a range of different levels, spanning topics such as protection of sensitive client data, managing cyber risk, the use of big data in marketing and pricing financial products, new methods of payment services, distributed ledger technologies, the creation and trading of virtual currencies, automated surveillance of trading activity, automated communications surveillance, and management of ABC, AML and sanctions risks. The impact of technology on the risks that we face and how we manage those risks has grown exponentially even in the last 10 years – and this shows no sign of abating.

On behalf of all of our global team, we hope that you enjoy reading our viewpoints on what lies ahead in 2020 and how best to tackle these new challenges. As always, please do get in contact if you have your own perspectives and thoughts on the issues that we have covered.

Kind regards

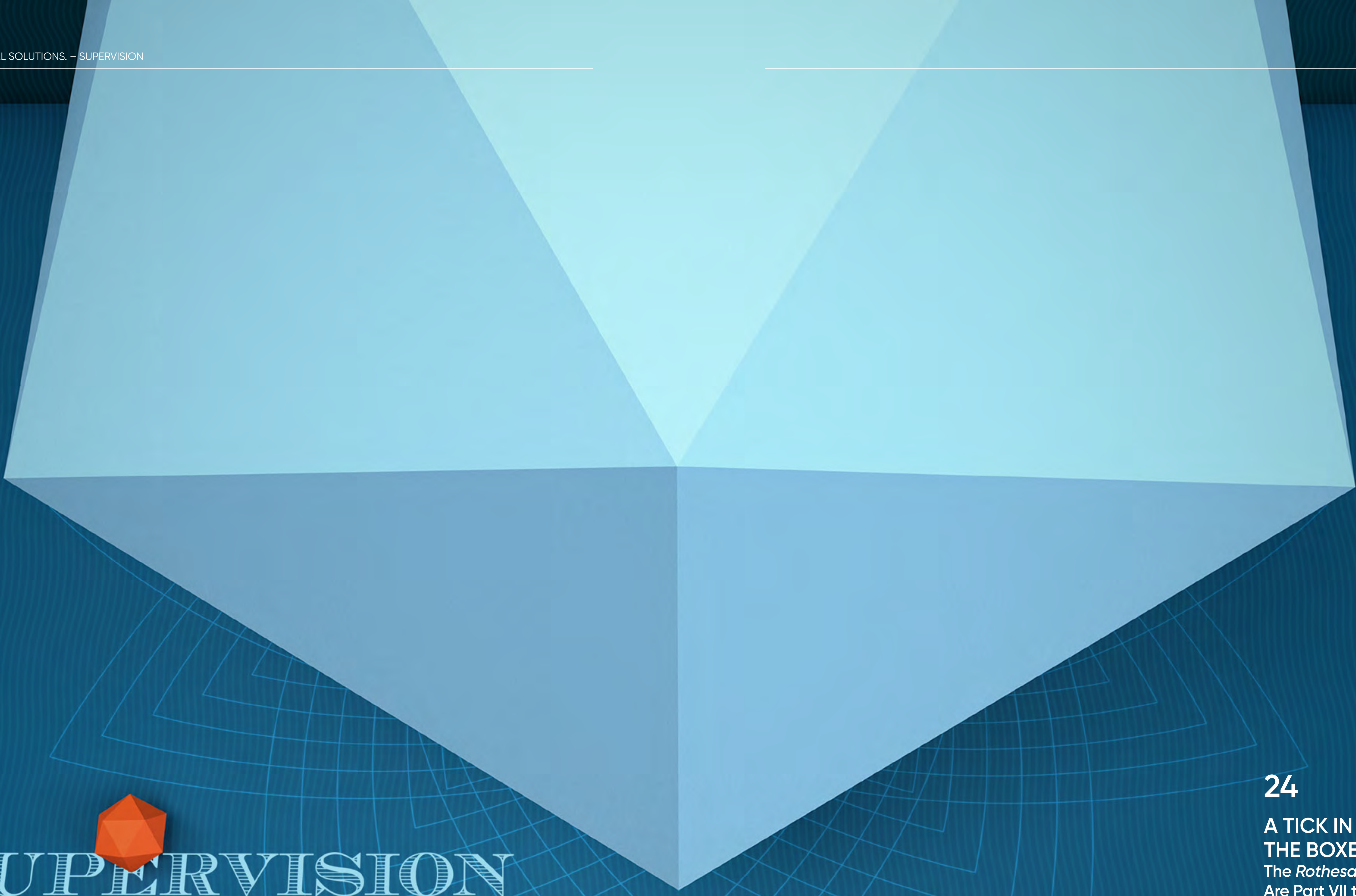
Nathan Willmott and Mark Srere

NATHAN WILLMOTT
Co-head of the Investigations, Financial Regulation & White Collar Group, London

MARK SRERE
Co-head of the Investigations, Financial Regulation & White Collar Group, Washington DC

[1] Still available online at https://www.bclplaw.com/en-GB/practices/emerging-themes-in-financial-regulation.html

CONTENTS



SUPERVISION

TELLING TALES OUT OF SCHOOL

WHEN DO YOU REPORT LOW-LEVEL MISBEHAVIOUR TO THE FCA?

Under the Senior Managers and Certification Regime ("SMCR"), firms are required to identify and report to the FCA any instances of disciplinary action taken in relation to conduct that would amount to a breach of one of the SMCR Conduct Rules. Almost all financial services workers are, or will soon be, within scope of the SMCR Conduct Rules (regardless of their seniority).

As the FCA seeks to use SMCR as a "lever" to drive culture change, firms must show they are implementing an appropriate framework for the identification and reporting of Conduct Rule breaches; and to minimise employment law risk, the framework should be fair to individuals.

ACCOUNTABILITY FOR ALL STAFF

The biggest change to individual accountability in the UK as a result of SMCR is the extension of personal regulatory accountability to all staff of regulated firms, save for "ancillary staff" (whose work is purely administrative).

The Conduct Rules under SMCR apply to all staff other than administrators, making the majority of financial services workers ("Conduct Rules Staff") directly accountable to the regulators for the first time. For banks, a handful of PRA-authorised investment firms and insurance companies, this is already the case. For firms regulated only by the FCA, the Conduct Rules were extended to their senior managers and certification staff in December 2019, and will apply to all of their Conduct Rules Staff from December 2020.

> "Under SMCR, any disciplinary action taken by a firm in relation to conduct that would amount to a breach of a Conduct Rule must be reported by the firm to the regulators"

Under SMCR, any disciplinary action taken by a firm in relation to conduct that would amount to a breach of a Conduct Rule must be reported by the firm to the regulators. The frequency of reporting varies according to the level of seniority of the individual who has been in breach, but the consequence is the same – a permanent regulatory black mark without a "sell-by" date, that is almost certain to route any future application by the person for approval to perform a controlled function into the dreaded "non-routine applications" sub-division (heralding longer timeframes, difficult questions asked and the risk of an embarrassing invitation from the regulator to one's employer to withdraw the application for approval). It is also a matter which the firm would be obliged to include on any regulatory reference, which could also damage the individual's future employability.

There have long been regulatory obligations to report any significant regulatory breach by a firm or its senior management – Principle 11 requires that anything of which the regulators would reasonably expect notice should be notified promptly to them.

> "The Conduct Rules breach reporting regime is less intuitive to implement in practice than the Principle 11 requirement, because there is no significance threshold attached to the new obligation to report"

The Conduct Rules breach reporting regime is less intuitive to implement in practice than the Principle 11 requirement, because there is no significance threshold attached to the new obligation to report – any misconduct for which a person has been disciplined (with the lowest threshold being the issuance of a formal written warning) is notifiable to the extent that it relates to conduct which would amount to a breach of a Conduct Rule.

Senior managers and certification staff
DEC 2019

WHAT WOULD AMOUNT TO A BREACH OF A CONDUCT RULE, AND WHO DECIDES?

Given the serious potential consequences for an individual's career, ensuring consistency in identifying reportable Conduct Rule breaches is both fundamentally important from a fairness perspective (and therefore for employment law risk), and very difficult to achieve in practice. The Senior Management Function holder who holds the Prescribed Responsibility for implementation of the Conduct Rules regime is ultimately accountable for achieving this.

How can it be achieved? In our view, it is important for consistency purposes that anonymised records are kept of why particular disciplinary incidents have been deemed reportable as Conduct Rule breaches, and others have not. We have also seen some good practice where firms' senior management meet to agree, in principle, what types of misconduct they would generally consider to breach a Conduct Rule, and which they would not.

> "Given the serious potential consequences for an individual's career, ensuring consistency in identifying reportable Conduct Rule breaches is fundamentally important from a fairness perspective"

DEC 2020
All Conduct Rules Staff

CONCLUSION

It is still early days for the Conduct Rule breach reporting regime, so one would hope that there is still a fairly forgiving approach by the regulators to firms who don't get it right all of the time. As SMCR beds in though, the FCA has higher expectations of firms, including that firms should use the process of embedding SMCR as a "lever" to drive cultural improvements e.g. by stamping out "non-financial misconduct" – see Catherine McGrath and Adam Turner's article at page 16 – which the FCA now says is "as important" to tackle as "financial" misconduct (e.g. market abuse).

In this context, in the coming year it will become increasingly important for firms to be able to show that there are strong systems and controls in place for the effective identification and timely reporting of disciplinary incidents that amount to breaches of the Conduct Rules, even where such breaches are not sufficiently serious to be deemed "significant".

POLLY JAMES
Partner,
London

JOSEPH NINAN
Associate,
London

"FAIR" PRICING OF FINANCIAL PRODUCTS

WILL THE FCA INTRODUCE AN EXPRESS REGULATORY DUTY OF FAIR PRICING?

Over the coming months, firms will have the opportunity to provide their input on the FCA's proposals for reshaping the regulatory landscape, including the Principles for Businesses, and I expect the question of how to regulate pricing practices to be one of the most significant and contentious areas of debate.

In October the FCA announced a wide-ranging consultation on its overall role as regulator, the outcomes that it should be seeking, and the consequent changes to its rules and guidance. It views this as a significant "opportunity to re-shape how financial services regulation works in the UK".

Of particular interest will be how far the regulator should intervene on the prices firms set for their products and services, and the methods used for setting those prices.

In the FCA's previous guise as the Financial Services Authority ("FSA") in the period 2001-2013, the regulator was at pains to make clear that it was not a price regulator. The FSA viewed the prices that firms set as outside the scope of its regulatory responsibilities, and did not view the prices charged as part of the "treating customers fairly" duty. The FSA would not step in simply to prevent the consumer making a bad bargain.

CHANGE OF MINDSET

Since its relaunch as (principally) a conduct regulator in 2013, the FCA has grown to view price-setting as squarely within its responsibilities. There are perhaps four main reasons for this change of mindset and approach from the regulator.

Firstly, in a handful of areas of potentially significant harm, Parliament has enacted discrete statutory duties requiring the FCA to regulate prices. As a consequence, specific restrictions have been introduced by the FCA on high-cost short-term credit in 2014, on workplace personal pension schemes in 2015 and on early exit pension charges in 2016.

Secondly, in April 2015 the FCA became a concurrent competition regulator, with additional powers and responsibilities for promoting effective competition in the financial services sector. In this new role, the FCA has a greater range of tools available to it to intervene in the structural aspects of markets – including pricing practices – to promote better competition.

Thirdly, the increasing prevalence of digitised sales has allowed for prices to be based on a wider range of factors than would historically have been the case, and which some may consider to be unfair to the consumer.

Finally, building on lessons learned from payment protection insurance mis-selling, the FCA has placed greater focus on product governance at the product provider, rather than focusing solely on the sales process followed by the customer-facing intermediary. The FCA has required product providers to consider the target market for its products and assess whether its products deliver a valuable service to consumers.

> "The FCA clearly now believes that the duty to treat customers fairly extends to a firm's approach to setting prices"

FAIR PRICING

The FCA's pricing focus has mainly been on the extent to which firms' pricing practices are "fair" to consumers, rather than the absolute price at which products are sold. The FCA now maintains that the Principle 6 duty to treat customers fairly extends to a firm's approach to setting prices. The FCA has particular concerns about "price discrimination" – the extent to which prices charged vary depending on factors which go beyond the cost of providing the product and the associated risk factors – for example, the practice of charging higher amounts to loyal customers who have remained with the product provider over the longer term.

Similarly, the FCA has concerns about firms offering products at a low initial cost, in the expectation that the consumer will forget to cancel the product when the price is raised in the future. Its concerns also extend to the utilisation by firms of additional (non core) factors in the pricing of a product for a particular individual, based on extra data available – such as how price-conscious the customer is likely to be.

> "The FCA has particular concerns about "price discrimination""

POWERS AND DUTIES

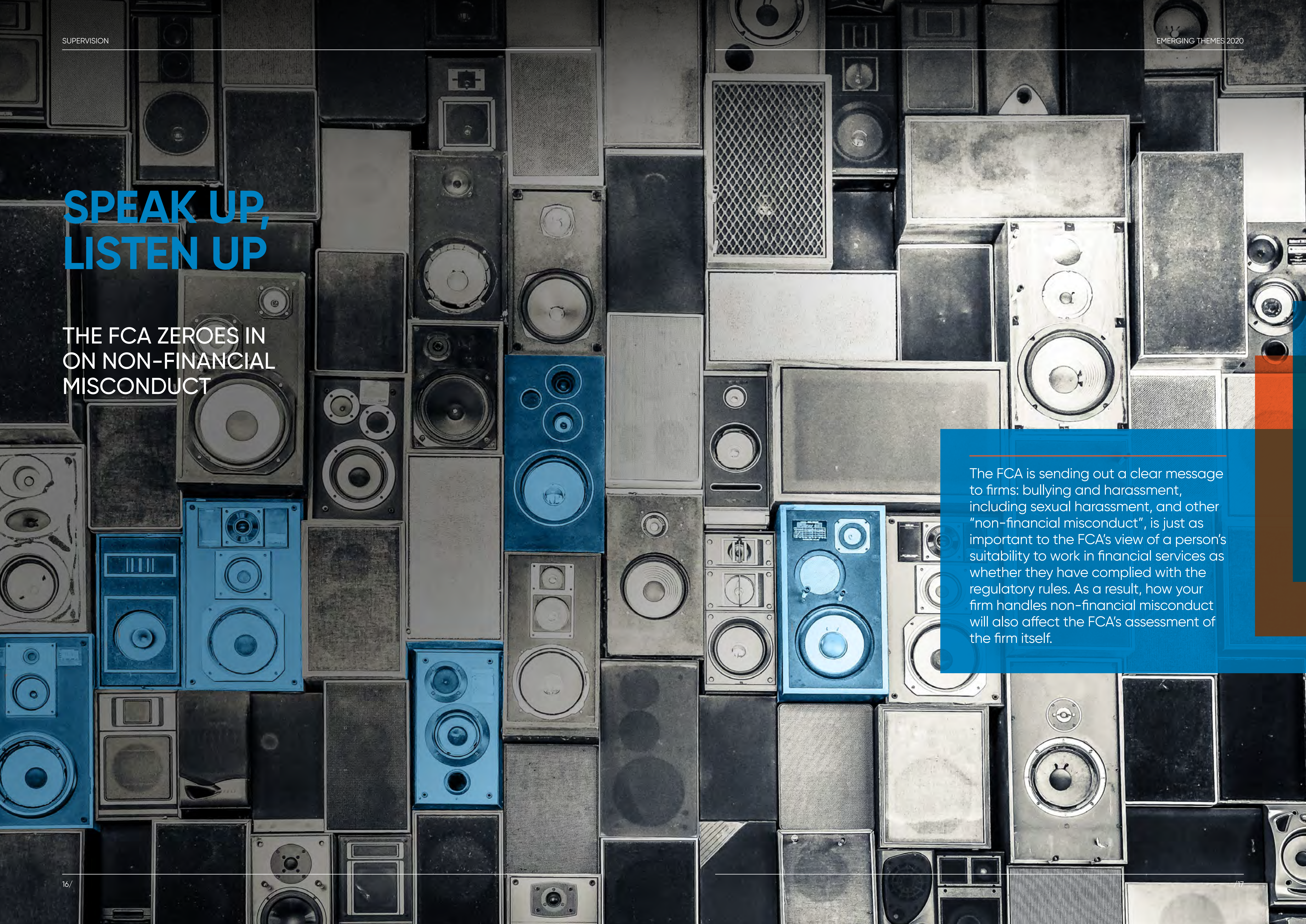
Outside the discrete price cap powers listed above, the FCA does not currently have clear powers to take action against firms who are perceived to be applying "unfair" pricing practices of this nature. It is arguable whether Principle 6 (paying due regard to the interests of customers and treating them fairly) on its proper interpretation does extend to how a firm sets its prices – the FCA cannot be confident that the Upper Tribunal would uphold such a wide definition of the duty.

CONCLUSION

I therefore expect that the regulator will seek to introduce more explicit new rules on how firms set their prices. As part of its ongoing review, I believe the FCA will add to its Principles for Businesses a specific duty on firms to adopt fair pricing practices.

Defining what "fair" looks like is not straightforward, and therefore I expect the FCA to fall back on the adoption of a high level obligation of this nature, with examples of good and bad practice in underlying guidance.

NATHAN WILLMOTT
Partner,
London



SPEAK UP, LISTEN UP

THE FCA ZEROES IN ON NON-FINANCIAL MISCONDUCT

The FCA is sending out a clear message to firms: bullying and harassment, including sexual harassment, and other "non-financial misconduct", is just as important to the FCA's view of a person's suitability to work in financial services as whether they have complied with the regulatory rules. As a result, how your firm handles non-financial misconduct will also affect the FCA's assessment of the firm itself.

CULTURAL TRANSFORMATION IN THE SPOTLIGHT

Poor culture was identified by the Parliamentary Commission on Banking Standards' 2013 report as a key root cause of conduct failings that have occurred in the last decade within financial services. As a result, the regulators have made it a priority to ensure that firms understand the importance of fostering the right culture within their businesses. At the same time as recognising the importance of culture, the regulators have been quick to admit that changing culture is no simple matter.

The FCA's focus on culture continues to evolve. One recent development is the broadening approach the FCA is taking to conduct regulation, particularly its focus on non-financial misconduct. This has been thrown into sharp relief by the #MeToo movement, which has put workplace sexual misconduct at the top of the agenda for many organisations, including in financial services.

The July 2018 Women and Equalities Committee's report on "Sexual harassment in the Workplace" was highly critical of the failure of government, regulators and employers to tackle workplace sexual harassment. The Committee emphasised the need for regulators to take a more active role in tackling harassment.

The FCA was quick to respond. In her letter to the Committee in September 2018, Megan Butler (Executive Director of Supervision, FCA), made clear that the FCA views sexual harassment as misconduct falling within the scope of its regulatory framework. She also said that it was relevant to individual fitness and propriety. Christopher Woolard (Executive Director of Strategy and Competition, FCA) elaborated further in December 2018 when he said that non-financial misconduct was misconduct "plain and simple" and that the way firms handle non-financial misconduct is as relevant to the FCA's assessment of the firm as their handling of financial misconduct.

PSYCHOLOGICAL SAFETY

The FCA's 2019/20 Business Plan highlights further developments in its approach. The FCA emphasised its concern that not only did #MeToo and other non-financial misconduct events continue to happen, but also expressed concern with the inadequacy or preparedness of managerial responses. In the FCA's view, these are clear symptoms of an unhealthy workplace culture – one which tolerates non-financial misconduct and doesn't encourage people to speak up, or to challenge decisions.

The emphasis on fostering a "speak up, listen up" culture – an environment of psychological safety where people feel able to express opinions in the workplace – marks a material evolution in FCA expectations. Whilst well implemented regulatory whistleblowing channels have been effective in enabling staff to raise reportable concerns without fear of unwanted identification or reprisal, they are not sufficient to embed a culture of openness. A healthy speak up culture reduces the need for people to feel they have to escalate issues via the whistleblowing channel or, for HR-focused issues, by raising a formal workplace grievance.

> "Although much of the focus to date has been on sexual misconduct and harassment, complaints of racism, homophobia, bullying or other discriminatory behaviours will be of equal interest to the regulators"

> "An environment of psychological safety where people feel able to express opinions in the workplace"

WHAT THIS MEANS FOR FIRMS

Firms are starting to recognise the importance placed by the regulators on non-financial misconduct. This is reflected in the noticeable increase in reports to the FCA concerning issues like discrimination and sexual harassment. Although much of the focus to date has been on sexual misconduct and harassment, complaints of racism, homophobia, bullying or other discriminatory behaviours will be of equal interest to the regulators.

Firms should review arrangements in place to ensure employees feel confident to raise issues as and when they arise, to embed this "speak up, listen up" culture. As the FCA points out, a key benefit of such an open culture is that firms may often be able to identify and act on issues at an earlier stage, before they have the potential to become very damaging.

When issues are raised, firms need to ensure they are appropriately investigated and, where necessary, action is taken. A well-founded complaint of non-financial misconduct committed by a senior manager or member of certified staff will require a review of whether that individual remains fit and proper to carry out their role.

Where a non-financial misconduct issue of sufficient materiality is raised, firms will need to assess whether they need to report the matter to the FCA/PRA. No firm can safely assume that the regulators would not want to know about non-financial misconduct in the current climate.

CATHERINE MCGRATH
Senior Associate,
London

ADAM TURNER
Associate Director,
London

SIZE MATTERS

NEW PRUDENTIAL FRAMEWORK FOR EU INVESTMENT FIRMS

The new Investment Firms Directive 2019/2034 ("IFD") and Investment Firms Regulation 2019/2033 ("IFR") were published in the Official Journal of the EU on 5 December 2019 and will apply (subject to local implementation of the IFD) from 26 June 2021.

The IFD/IFR will introduce a new prudential regime for EU investment firms authorised under the Markets in Financial Instruments Directive ("MiFID II"). The UK government has indicated that it intends to implement the IFD/IFR, although the uncertainty over Brexit has left the exact position unclear.

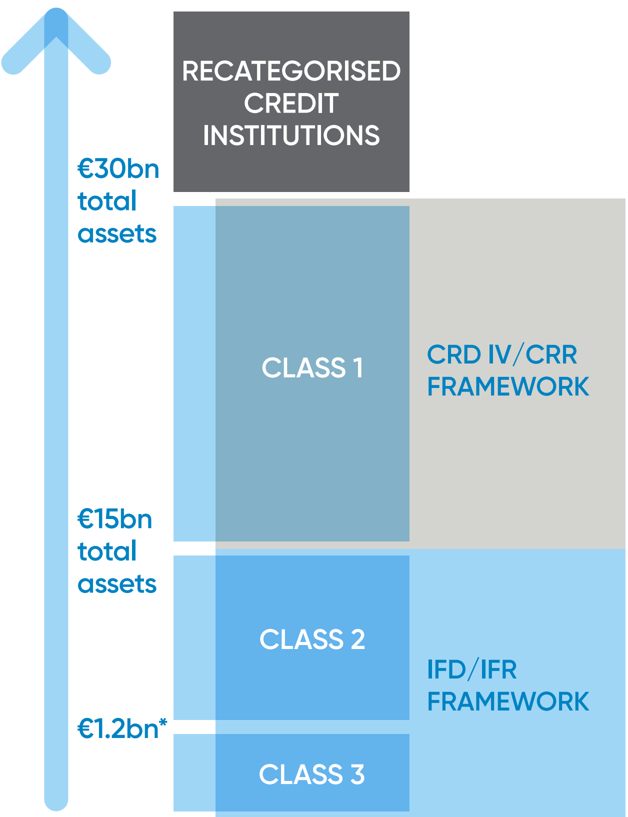
SCOPE

EU investment firms are currently subject to the prudential requirements under the Capital Requirements Directive and the Capital Requirements Regulation ("CRD IV"/"CRR"[1]). The IFD/IFR will change that.

The IFD/IFR categorise investment firms into three classes:

- Class 1 covers firms that conduct underwriting business and proprietary trading and have assets exceeding €15 billion. However, those with assets exceeding €30 billion will be re-classified as "credit institutions" (i.e. no longer "investment firms")
- Class 3 firms are those that meet specified criteria (e.g. balance sheet below €100 million, gross revenue below €30 million and assets under management below €1.2 billion)
- All other investment firms are class 2 firms.

NEW CATEGORISATION



* Assets under management and other criteria.
[1] CRD IV/CRR have been amended by CRD V/CRR II. The changes (mainly for credit institutions) are not discussed here.

OVERVIEW

The IFD/IFR will apply in their entirety to class 2 firms. Class 3 firms will be subject to lighter requirements within the new framework. Class 1 firms will largely remain under the CRD IV/CRR framework and are thus not further discussed here.

REGULATORY CAPITAL

The IFD/IFR increase the current minimal capital requirements by €20,000/€25,000. However, since the ongoing capital that most investment firms are required to maintain tends to exceed such capital floors, the impact of such increases may largely be inconsequential.

Broadly, class 2 firms need to calculate their regulatory capital by reference to specified "K-factors" which are designed to reflect the risk profiles of investment firms. The regulatory capital for class 3 firms is essentially 25% of their annual fixed overheads, similar to the current requirement for relevant firms.

During a five-year transition period, investment firms can cap their capital under the new rules to twice the amount calculated under the current CRD IV/CRR rules.

REMUNERATION REGIME

While most of the new remuneration requirements are similar to the current CRD IV/CRR rules, they are generally less stringent. For example, the IFD/IFR do not contain the 200% bonus cap under CRD IV/CRR. The IFD/IFR remuneration disclosures are also less extensive. Class 3 firms only need to comply with the much lighter MiFID II remuneration requirements.

POTENTIAL IMPACT

The IFD/IFR essentially categorise investment firms according to their systemic risk, whereas CRD IV/CRR differentiate investment firms by the particular type of MiFID II activities they undertake. Consequently, it seems futile to map the new classes to the current categories; the European Banking Authority has identified 11 different types of investment firms under the current framework. Subject to the local implementation of the IFD/IFR, each firm will have to assess which new class it would fall into.

In the UK, there are three broad groups of investment firms: IFPRU firms, BIPRU firms and IFPRU firms that are dual regulated by the FCA and the PRA; there are sub-categories under each.

FCA/PRA dual-regulated IFPRU firms may likely fall within class 1 (some may be re-categorised as credit institutions). Certain larger IFPRU firms that are solo-regulated by the FCA (i.e. not large enough to be dual-regulated) may also fall within class 1. These firms should see minimal changes as they would essentially remain within the current CRD IV/CRR regime.

BIPRU firms and some (smaller) IFPRU firms may fall within either class 2 or class 3; most BIPRU firms may fall within class 3. The impact may vary, given the complexity of the current rules as applicable to different sub-categories of BIPRU firms; generally, the new requirements should be less burdensome (which is one of the objectives of the IFD/IFR).

The situation may well be different in other member states.

> The various technical standards required by IFD/IFR may not be finalised until the second half of 2020

CONCLUSION

While the IFD/IFR aim to streamline and harmonise the current rules which are considered unduly complex for investment firms, they provide for various discretions to EU member states. The impact will depend on the local implementation of not only the new IFD/IFR but also the current CRD IV/CRR.

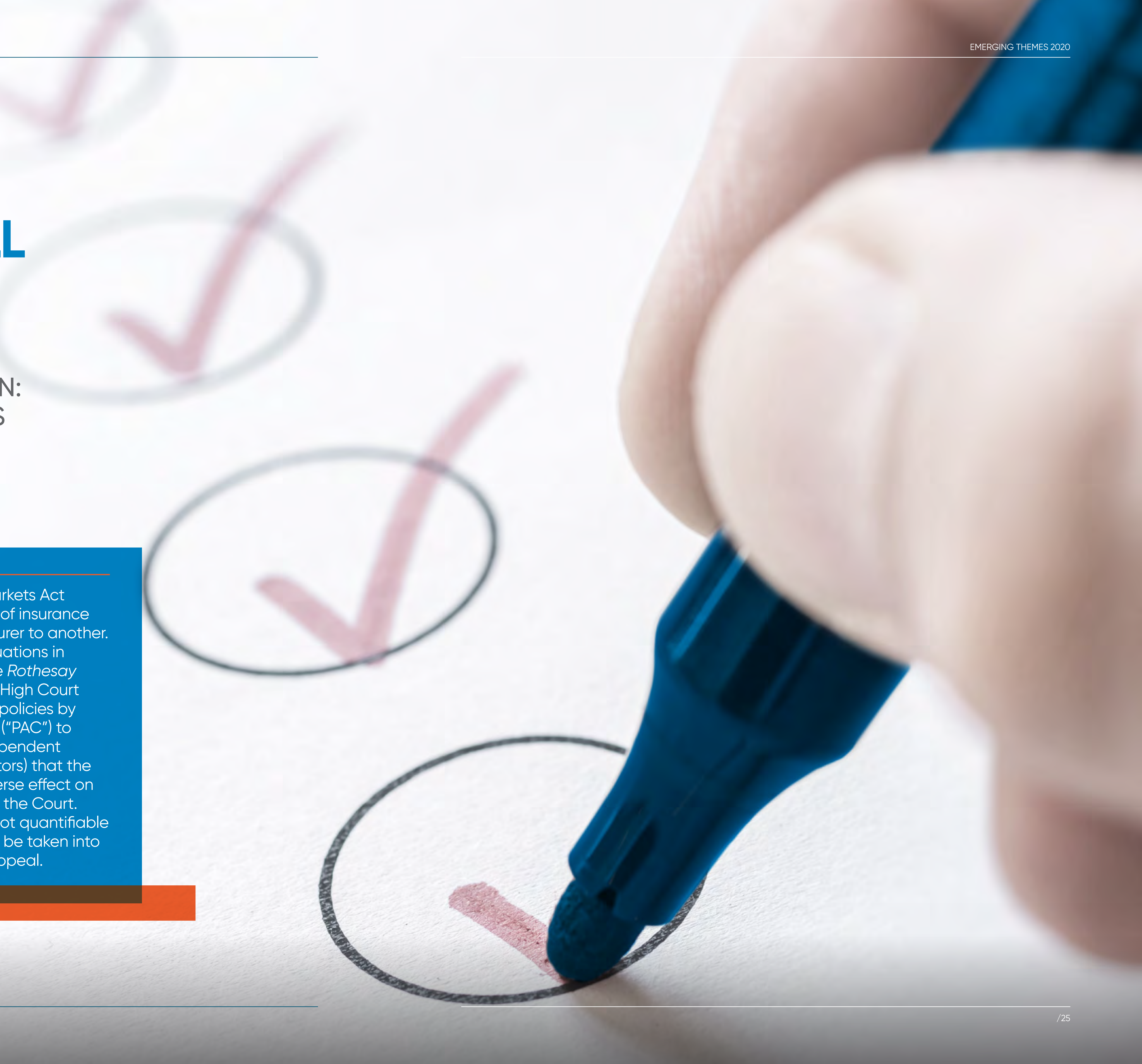
The implementation timeline may be challenging, particularly given that various technical standards required by IFD/IFR may not be finalised until the second half of 2020. It is therefore advisable that investment firms start preparation sooner rather than later, particularly for those that will fall into classes 1 or 2.

KAI ZHANG
Associate Director,
London

A TICK IN ALL THE BOXES

THE *ROTHESAY* DECISION: ARE PART VII TRANSFERS NOW RESTRICTED?

Part VII of the Financial Services and Markets Act 2000 is the mechanism by which books of insurance policies can be transferred from one insurer to another. Some doubt has been cast over the situations in which this process can be utilised by the *Rothesay* decision in August 2019. In this case, the High Court blocked a proposed transfer of annuity policies by Prudential Assurance Company Limited ("PAC") to Rothesay Life plc ("Rothesay"). The Independent Expert's view (undisputed by the regulators) that the transfer would not have a material adverse effect on policyholders was not enough to satisfy the Court. However, the judge said other factors, not quantifiable by an actuary or regulators, also had to be taken into account. The parties have lodged an appeal.



370k Annuity policies £12bn

£508bn Prudential Group

£37bn Rothesay

THE PROPOSED TRANSFER

The proposed transfer involved around 370,000 annuity policies with estimated liabilities of £12 billion. There were to be no changes to policy terms, and the policies would continue to be administered (at least initially) by the existing service provider.

VALUE OF THE INDEPENDENT EXPERT AND REGULATORS' CONCLUSIONS

While it has always been clear that Court approval for a Part VII transfer is not a rubber stamp, it is highly unusual for a transfer to fail if, as in this case, neither the Independent Expert nor the regulators identify any issues with it. Mr Justice Snowden felt that the Independent Expert's and the regulators' analyses were limited to actuarial and Solvency II regulatory principles, and the Court should take account of broader questions.

THE COURT'S APPROACH

In line with earlier cases, Mr Justice Snowden's stated approach was to strike a balance between the parties' commercial rationale and policyholder interests. However, some of the factors he took into account were not obviously directly relevant to the impact of the transfer on policyholders. These included:

- Policyholders originally chose PAC for its age and established reputation. Rothesay, a relative newcomer, did not share those attributes
- It was reasonable for policyholders to assume from PAC's literature that it would not seek to transfer their policies
- PAC had already achieved its commercial objective of releasing regulatory capital to support a proposed demerger through a pre-transfer reinsurance with Rothesay.

Mr Justice Snowden was also influenced by the relative size of the parties – the Prudential Group has assets of £508 billion, compared to Rothesay's post transfer asset base of £37 billion – and the fact that annuity policies may provide the only source of income for a policyholder.

IS LACK OF ADVERSE IMPACT NO LONGER ENOUGH?

The Court's approach to date has always been to determine whether the transfer will have a material adverse effect on policyholders and to have regard to real, not fanciful, risks. Mr Justice Snowden however was influenced by the fact that PAC had qualities (longevity and reputation) not shared by Rothesay; and by the impact on policyholders if Rothesay should fail, even though the Independent Expert considered the risk remote.

> "The Court's approach to date has always been to determine whether the transfer will have a material adverse effect on policyholders and to have regard to real, not fanciful, risks"

The judge's approach seemed to be that if the transferor would be better able to withstand a shock than the transferee, the transfer ought not to be sanctioned. This differs from the previous approach that if the transferee is financially strong, it should not matter that the transferor has more assets. Mr Justice Snowden acknowledged his view might have been different if PAC's commercial purpose for the transfer was different; the transfer was proposed to policyholders on different terms; or, if there was less disparity between the transferor and transferee in the characteristics policyholders consider important when selecting an annuity provider.

If Mr Justice Snowden's approach is correct, an insurer would need to find a counterparty that is not just financially strong, but has the same financial strength, longevity and reputation as the transferor. This significantly reduces the pool of potential acquirers. It could also make it difficult for a specialist run-off acquirer to take on even a relatively small book from a substantial live underwriter. This could have the effect of almost entirely undermining the purpose of Part VII transfers.

> "The judge's approach seemed to be that if the transferor would be better able to withstand a shock than the transferee, the transfer ought not to be sanctioned"

CONCLUSION

Just two months after the *Rothesay* decision, in October 2019 Mr Justice Morgan sanctioned "without hesitation" a Part VII transfer of insurance business in *Re Canada Life Ltd.* The *Rothesay* decision in his view was clearly distinguishable. There were proper commercial reasons for the transfer. Canada Life wanted to divest itself of a non-core business, and was disposing of it to a specialist provider actively focused on that business. Mr Justice Morgan held that was likely to be of real benefit to policyholders.

If a clear benefit to policyholders can be shown, *Rothesay* should not be an issue, but simply showing that there is no financial prejudice to policyholders may no longer be sufficient.

ANTHONY LENNOX
Partner,
London

OLIVER SAUNDERS
Senior Associate,
London

A CALL TO ACTION

CUSTOMER VALUE IN THE GENERAL INSURANCE DISTRIBUTION CHAIN

In its thematic review of general insurance distribution chains, the FCA expressed extreme disappointment at a widespread industry failure to focus on customer outcomes in the approach to product development and distribution. It expects firms urgently to address failures in culture and governance and achieve a step change in their approach. The FCA is very clear that it will not hesitate to intervene using the full range of its regulatory tools where it identifies failings.

WHAT HARMS HAS THE FCA IDENTIFIED?

Two main areas of potential harm were identified:

- Price and quality
  - Sub-standard or low quality products
  - Excessive fees and charges affecting customer value.
- Sales and customer service
  - Sales of unsuitable products not consistent with the customer's needs
  - Failure to fulfil obligations to customers, such as claims handling, promptly and to the appropriate standard
  - Unavailability of services, because of system failures or cyber issues.

WHAT ARE THE KEY CAUSES?

According to the FCA, the key causes are:

- Purpose and values – firms having business models and strategies characterised by a lack of focus on customer outcomes
- Poor governance and oversight – failure to have adequate systems and controls over the end to end product and service development, manufacture and delivery chain.

These issues are exacerbated by the increasing length and complexity of distribution chains. The FCA seems concerned in particular that firms do not have sufficient oversight of unregulated distributors, and are not complying with their Insurance Distribution Directive obligations to ensure sales through unregulated parties meet the required standards. The FCA comments on the potential for chains to be influenced by parties who are not FCA regulated, like large retailers.

EXPECTATIONS OF MANUFACTURERS

The FCA expects manufacturers to have a product approval process covering design and review, which considers the value the product presents for the target market and how the distribution chain affects value. By "value" the FCA means cost to the customer and compared to quality of both the product and services.

Firms should use their own customer research, claims and complaints data and external information like analysis of competitor products, to assess value at the design stage. They

> "The FCA expects manufacturers to have a product approval process covering design and review"

should consider the difference between the risk price and the end premium, including commission received by other parties in the chain; and, where they can reasonably obtain it, information on fees charged by those parties.

Where potential poor value is identified, firms should consider what other information they can reasonably obtain to determine whether there is harm to customers. This might include cost/remuneration information from other parties in the chain (bearing in mind wider legal obligations including competition law) and details of the role of each party, to assess whether remuneration is justified.

Manufacturers should carry out ongoing product reviews, and ensure they have management information to help them assess product value and the impact of the distribution chain. Where products are detrimental to customers, manufacturers must have processes in place to mitigate and remediate harm. This may mean withdrawing the product from the market or significantly changing the distribution method.

EXPECTATIONS OF DISTRIBUTORS

The FCA expects distributors to be able to identify signs that a product is not delivering its expected value through direct interactions with customers, assessments of customers' demands and needs, analysis of claims and complaints and referencing FCA published data on value measures in general insurance.

Where they identify that a product is detrimental they are expected to amend distribution, for example, by stopping the use of particular distribution methods, reducing the amount of remuneration they receive or ceasing to distribute the product.

Distributors must understand the manufacturer's assessment of the expected value of the product and ensure that remuneration arrangements do not erode that value or conflict with the customer's best interests rule. Where there is a conflict (for example because remuneration bears no reasonable relationship to the distributor's costs or workload) the arrangement must be changed. Unlike other cases of conflict, disclosure is not sufficient to address the issue.

Distributors are expected regularly to review their distribution process to ensure it is not detrimental to customers, for example, by reaching customers outside the target market or to whom it does not provide value. Distributors must provide manufacturers on request with appropriate information on the results of their reviews and with sales information, to support the manufacturer's product reviews. They must also have adequate systems and controls over delegated activities.

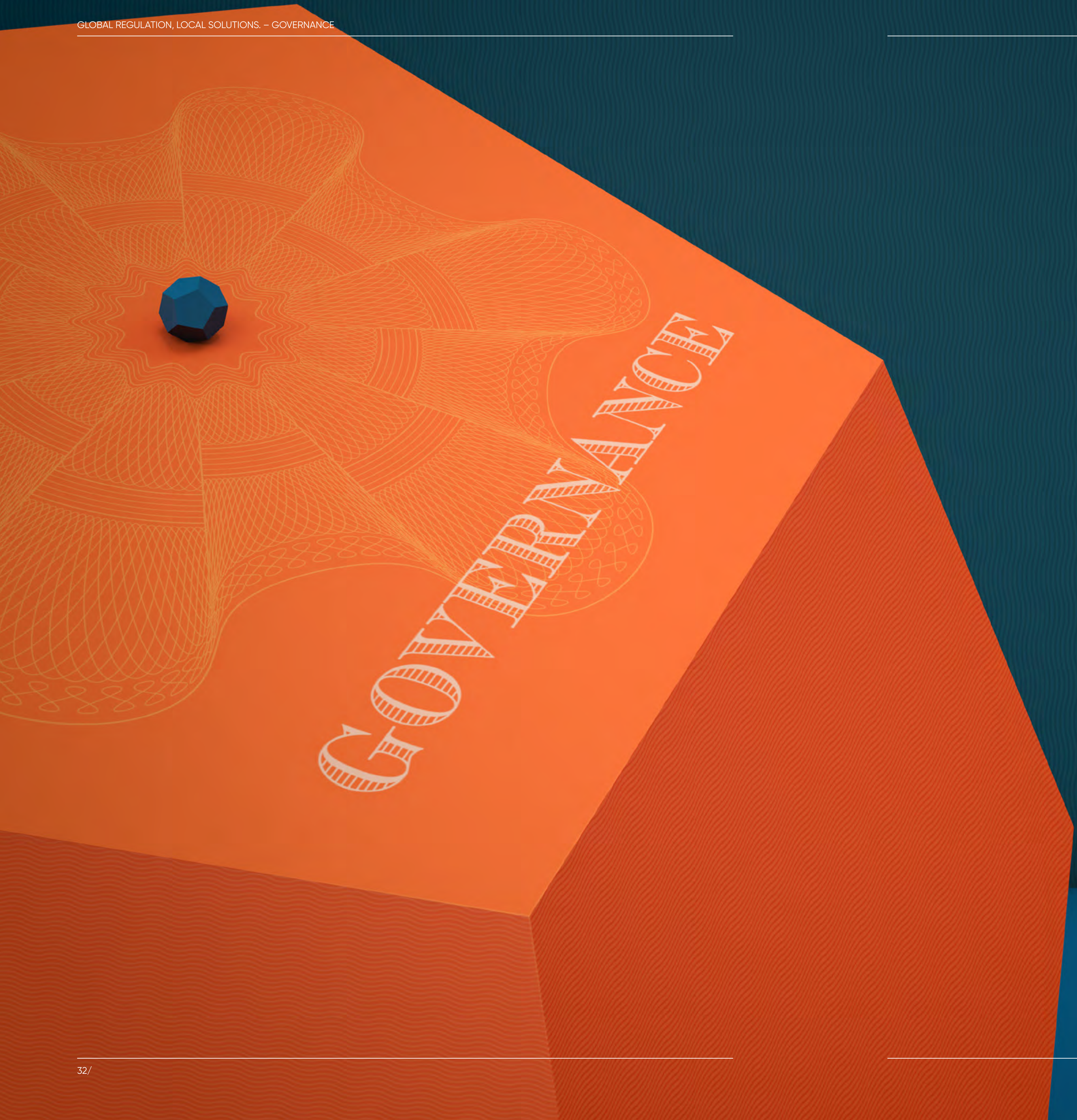
> "The FCA clearly feels that firms have not taken enough action to address concerns previously raised"

GERALDINE QUIRK
Partner,
London

LAURA JACKSON
Associate,
London

CONCLUSION

The FCA clearly feels that firms have not taken enough action to address concerns previously raised by it, including in its 2015 report on delegated authorities. The FCA's finalised guidance is designed to remove any ambiguities around its expectations, and to make it easier to intervene where it identifies failings. Firms should ensure they are ready to demonstrate that their design and distribution processes protect customers from the potential harms the FCA identifies.

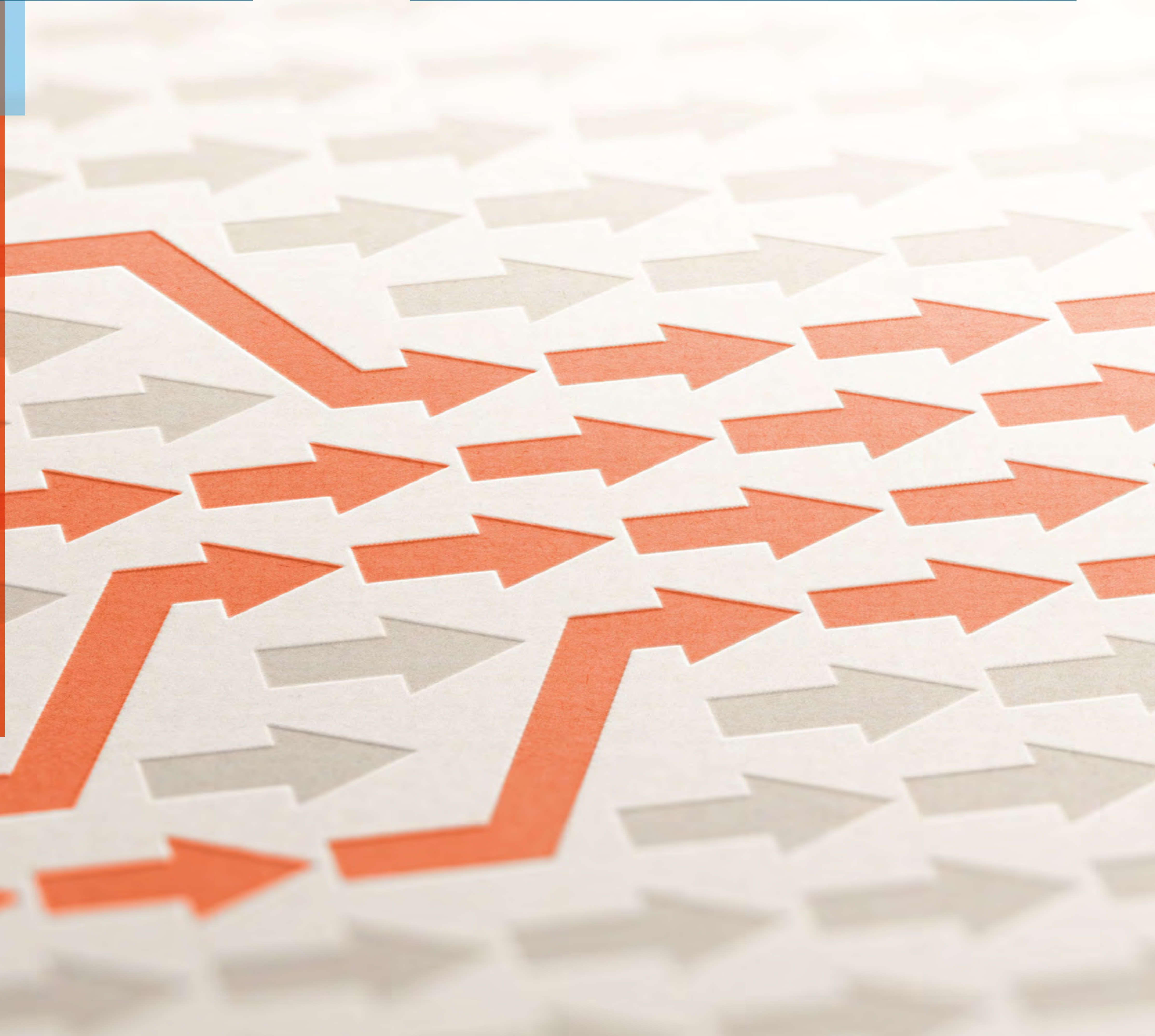

GOVERNANCE

GET ON TRACK FOR SMCR

THE JOURNEY FOR SOLO-REGULATED FIRMS

All UK authorised firms that are solo-regulated by the FCA will be fully within the scope of the Senior Managers and Certification Regime ("SMCR") from 9 December 2020, following a staggered implementation period which started on 9 December 2019.

In the year ahead it is therefore vital for firms to understand the key changes as a result of the SMCR for solo-regulated firms, and to put in place an implementation plan.



PERSONAL REGULATORY DUTIES FOR EVERYBODY

The extension of personal regulatory duties beyond approved persons will feel like the most significant change for most people at solo-regulated firms, many of whom have never been accountable directly to regulators for their personal conduct. This needs careful explanation and messaging to staff.

For solo-regulated firms, the FCA's Conduct Rules currently apply only to Senior Management Function ("SMF") holders, non-executive directors and certification staff. From 9 December 2020, the Individual Conduct Rules will apply to all staff (except those carrying out purely administrative roles specified in the FCA's rules). Failure to meet the standards imposed under the Conduct Rules will mean that an employee could be liable to regulatory enforcement action, including a financial penalty.

Firms have a statutory obligation under the new regime to provide training to employees within scope of the Conduct Rules, to help them understand their personal regulatory duties. This training must be provided by 9 December 2020. Firms also need to have processes to train new joiners and provide periodic refresher training.

In the post-SMCR world, solo-regulated firms must also notify the FCA if they take disciplinary action (which includes issuance of a formal written warning) against a person relating to any action, failure to act, or circumstance that amounts to a breach of any of the Conduct Rules. Please see Polly James' and Joseph Ninan's article for commentary on the challenges associated with these new reporting requirements.

THE NEW CERTIFICATION REGIME

The new Certification regime requires solo-regulated firms to identify which of their staff are performing specific FCA certification functions, and to assess the fitness and propriety of each individual to perform their roles, on an annual basis.

If, for whatever reason, a certification staff member cannot be certified as fit and proper to perform their role at the annual certification deadline, they will need to be removed from their role or temporarily re-deployed. Regulatory references will also need to be obtained for new certification staff (i.e. those who were not already in role at the time of commencement) and firms will be required to have a written policy in place, showing how they comply with the FCA's regulatory reference requirements.

Solo-regulated firms were required to identify and provide Conduct Rules training to their certification staff by 9 December 2019, and must now put in place a process to certify them as fit and proper by 9 December 2020.

From our experience in advising banks and insurers on the first wave of SMCR implementation, the certification regime is likely to result in the need to make various amendments to HR policies and procedures (including any fit and proper policy, appraisal forms, assessment records and/or employment contracts). It may also require difficult judgment calls to be taken in the event that there are questions over an individual's fitness and propriety – it is worth thinking through in advance some scenarios where this may arise.

> "From 9 December 2020, the Individual Conduct Rules will apply to all staff"

ARE YOU ON TRACK TO BE SMCR-READY?

I have set out below three key questions that I feel that solo-regulated firms should be asking themselves when assessing whether they are on track to be SMCR-ready by 9 December 2020:

- **Have you identified all your certification staff** and are you putting in place a process to assess their fitness and propriety? Remember, you have a year until December 2020 to devise and implement a certification process (to cover both existing staff and new joiners)
- **Have you identified your Conduct Rules staff** who come into scope of the new rules on 9 December 2020, and do you have plans to ensure they receive tailored training on the Conduct Rules before that date (including planning for refresher training and training for new staff members)?
- **Do you have suitable policies in place to evidence your processes** (e.g. a regulatory reference policy and a Conduct Rules training/breach reporting policy)? This will help to protect SMFs with prescribed responsibilities relating to SMCR compliance.

CONCLUSION

From our experience, implementing these requirements takes longer and is more complex than you may think. Our advice is to start as soon as you can to ensure you are ready by the December deadline.

ADAM JAMIESON
Senior Associate,
London

> The regime is intended to quickly identify individuals to whom supervisory concerns can be communicated, and of course to make them accountable

DON'T DROP THE M-I-C

NOTIFYING THE HONG KONG SFC OF MANAGER-IN-CHARGE CHANGES

It is now over two years since the "Manager-in-charge of Core Functions" regime was implemented in Hong Kong by the Securities and Futures Commission ("SFC"). By raising the accountability of senior management, including directors, responsible officers and now the manager-in-charge, the regime aims to strengthen regulatory oversight of all SFC licensed corporations. It shares similarities with the Senior Managers and Certification Regime in the UK and the proposed guidelines on Individual Accountability and Conduct in Singapore.

SFC licensed companies should identify an individual as the manager-in-charge to be responsible for each of eight designated core functions:

(1) Overall Management Oversight

(2) Key Business Line

(3) Operational Control and Review

(4) Risk Management

(5) Finance and Accounting

(6) Information Technology

(7) Compliance

(8) Anti-Money Laundering and Counter-Terrorist Financing.

At the Hong Kong SFC Compliance Forum 2019, the SFC stated the regime is intended to quickly identify individuals to whom supervisory concerns can be communicated, and of course to make them accountable for control failures or conduct issues within the firm. Detailed risk assessments and clear understanding of your area of responsibility reduce the chance of personal sanctions in the event that breaches occur.

From the firm's perspective, care should be taken to define responsibilities clearly, especially where an individual is responsible for more than one core function. Consideration will need to be given to the rise of responsibilities falling between the gaps of core functions, for example outsourced services.

The firm should also ensure it creates an internal system to notify the SFC of any changes to manager-in-charge appointments or organisational charts within the specified time limits.

The regime's reach extends beyond Hong Kong and to companies that are not regulated by the SFC. For SFC licensed companies who are part of a wider group, information about individuals from other group companies (both within or outside Hong Kong) that are not regulated by the SFC may need to be submitted. As a starting point, firms need to map their governance and reporting structure to determine which businesses operate in which legal entities.

> The regime's reach extends beyond Hong Kong and to companies that are not regulated by the SFC

The Hong Kong SFC has been actively revamping its licensing processes to strengthen its gatekeeping function, and therefore compliance with the regime should not be taken lightly. However, the scale of any penalty remains fairly light – if a SFC licensed firm does not fulfil its duties under the manager-in-charge regime, a maximum fine of HK$50,000 may be imposed.

In the coming year, the SFC will be publishing more information on its enforcement actions, such as the types of firms targeted and the types of deficiencies. Firms need to stay alert to get a better idea of the SFC's focus within the regime.

GLENN HALEY
Partner,
Hong Kong

IAN CHENG
Associate,
Hong Kong

VIVICA FU
Trainee Solicitor,
Hong Kong

DON'T SHOOT THE MESSENGER

PREPARING FOR NEW WHISTLEBLOWING PROTECTION LAWS IN THE UAE

New laws in the UAE, as in a growing number of jurisdictions, are resulting in firms being subjected to increased scrutiny on how they engage with whistleblowers. To protect themselves in the year ahead, firms need to be aware of the new rules and take active steps to implement the regime and manage their regulatory risk.

WHAT'S CHANGED?

The whistleblowing landscape has changed in the UAE following the introduction by the Dubai International Financial Centre ("DIFC") of a new whistleblowing protection law, the DIFC Operating Law (DIFC Law No. 7 of 2018).

The new DIFC law includes protections for those blowing the whistle in relation to breaches of the Operating Law, its Regulations and any other legislation administered by the DIFC Registrar of Companies. This would, for example, include the DIFC Companies Law (DIFC Law No. 5 of 2018) and the DIFC Limited Partnership Law (DIFC Law No. 4 of 2006).

In particular, whistleblowers cannot be dismissed from employment or otherwise subjected to victimisation by the employer or any related person. Financial penalties can be imposed if firms breach these requirements, which of course would be in addition to any reputational impact.

KEY STEPS FOR EFFECTIVE COMPLIANCE

Key steps that firms based in the DIFC should be taking now, if they have not already done so, include:

- **Gap analysis** – review current policies and procedures against the new requirements. This may necessitate the creation of a whistleblowing policy and revisions to contracts of employment. Firms may consider engaging external service providers (e.g. whistleblowing hotlines), to provide a useful defence if the measures are later questioned.
- **Training** – firms should consider the method, timing and frequency of their training, tailoring it for different audiences (e.g. for managers receiving whistleblowing reports, and for staff running the firm's whistleblowing procedure).
- **Prepare for increasing numbers of whistleblowing investigations** – inevitably the new whistleblowing protections will lead to increasing numbers of disclosures requiring investigation. The general trend towards increased individual accountability in sectors such as financial services, also drives increased whistleblowing.
- **Prepare for complexity** – whistleblowing investigations can often be complex, time-critical and labour-intensive. Issues to consider include: preserving evidence; identifying and reviewing relevant correspondence/documents; interviewing the whistleblower and other relevant individuals; privilege and confidentiality, particularly in relation to the protection of the whistleblower; whether a report is needed (with conclusions and/or recommendations); and considering whether any formal legal or regulatory notification is required.

Where issues raised by a whistleblower have an impact on other jurisdictions as well as the DIFC itself, it will be critical to analyse how best to collect the facts and manage the interests of the variety of relevant regulators. For further discussion of the issues than can arise in these circumstances, see the article "BUILDING BRIDGES" on page 48.

RAZA MITHANI
Partner,
Dubai

GREEN BECOMES TRANSPARENT

ESG AND SUSTAINABLE GROWTH FIND REGULATORY CLARITY

Last year saw a real focus on the importance of sustainability in business activities, highlighted by the dramatic and very direct Extinction Rebellion campaign, the UN's Climate Action Summit in September and the high profile actions of individuals such as Greta Thunberg. After a relatively slow start, the financial services industry is beginning to acknowledge the importance of sustainability in its dealings with clients and investors, and in the development of product ranges. 2020 is likely to see that pace increasing further with a number of measures being taken at the national and international level.

As policymakers have become more interested in how asset managers achieve their non-financial goals, we are seeing a long-term trend emerge of environmental, social and governance ("ESG")/sustainable, responsible and impact investment ("SRI") standards driving regulatory compliance. ESG and SRI are also beginning to influence standards of care, with investors and lenders increasingly using ESG/SRI measures to evaluate the performance of investments. Asset managers who implement their commitment to sustainability and who hold consultants, managers and advisors to account, are likely to create a competitive advantage for themselves – and a "sustainability multiplier effect" in the market.

> "This legislation has a much shorter implementation period than most other EU financial services legislation, with affected firms only having 15 months to become compliant"

LEGAL AND REGULATORY ENVIRONMENT

There is strong political drive for responsible and sustainable business conduct – in the UK, EU-wide and globally. The UK backdrop, alongside various industry-led initiatives, includes the FCA's support for introducing climate-related mandatory disclosure requirements for regulated firms (as set out in its October 2019 Feedback Statement on Climate Change and Green Finance), and the Department for Work and Pensions' recommendation that pension scheme trustees prepare an optional policy on how investment strategies consider non-financial factors, such as ethics, social and environmental impact, and quality of life.

In November 2019 the EU adopted a package of measures on sustainable finance. The reform's key tenets are taxonomy, disclosure, investor duties, benchmarks and suitability. Asset managers will be required to integrate sustainability risks into their operating models, provide more detailed disclosures on ESG policies and sustainability risks and increase due diligence on the ESG profile of funds.

This legislation has a much shorter implementation period than most other EU financial services legislation, with affected firms only having 15 months to become compliant (with an additional year for the first annual reports containing ESG/sustainability information). Given this short window firms will need to begin their implementation planning early in 2020. Further, as EU delegated legislation is expected to impact MiFID II and IDD suitability testing, firms should also be prepared to take ESG considerations and preferences into account in the suitability assessments they undertake to see if proposed investments are appropriate for a client.

Investors and managers are already committing to aspirational and voluntary investment principles to mandate a more systematic approach to ESG integration into investment, risk and organisational processes. A growing number are signatories to the UN Principles for Responsible Investment. This involves a manager's commitment to six voluntary and aspirational investment principles, including: considering ESG issues when making investment decisions; seeking disclosures from ESG entities in which they invest; and reporting on ESG activities.

Side letter provisions are becoming more common, for instance that the manager maintains and/or introduces appropriate ESG strategies to the management of portfolio investments. Another framework recently consulted on, and which may become increasingly recognised by the funds industry, is the Sustainable Development Goals ("SDG") Impact Practice Standards for Private Equity Funds. This UN initiative provides a practical end-to-end checklist designed to integrate impact into fund design and execution.

> "The new taxonomy should give greater transparency for end-investors, allow better comparison between products and reduce opportunities for "green-washing""

CLARITY AND CHALLENGES

Policymakers are keen to provide clarity on what sustainable investments are by creating an EU-wide classification system to provide a common language to identify economic activities that can be considered environmentally sustainable. The new taxonomy should give greater transparency for end-investors, allow better comparison between products and reduce opportunities for "green-washing". Although this taxonomy is EU-centric and only likely to be mandatory for products that are marketed as a "sustainable investment", we expect it to become the global language of mainstream impact investment.

Regulatory consistency across the various standards, to avoid duplication or divergence, is key. Other challenges include specifying appropriate time horizons (particularly since many climate-related risks may crystallise beyond a firm's typical planning horizon) and modelling and methodological difficulties.

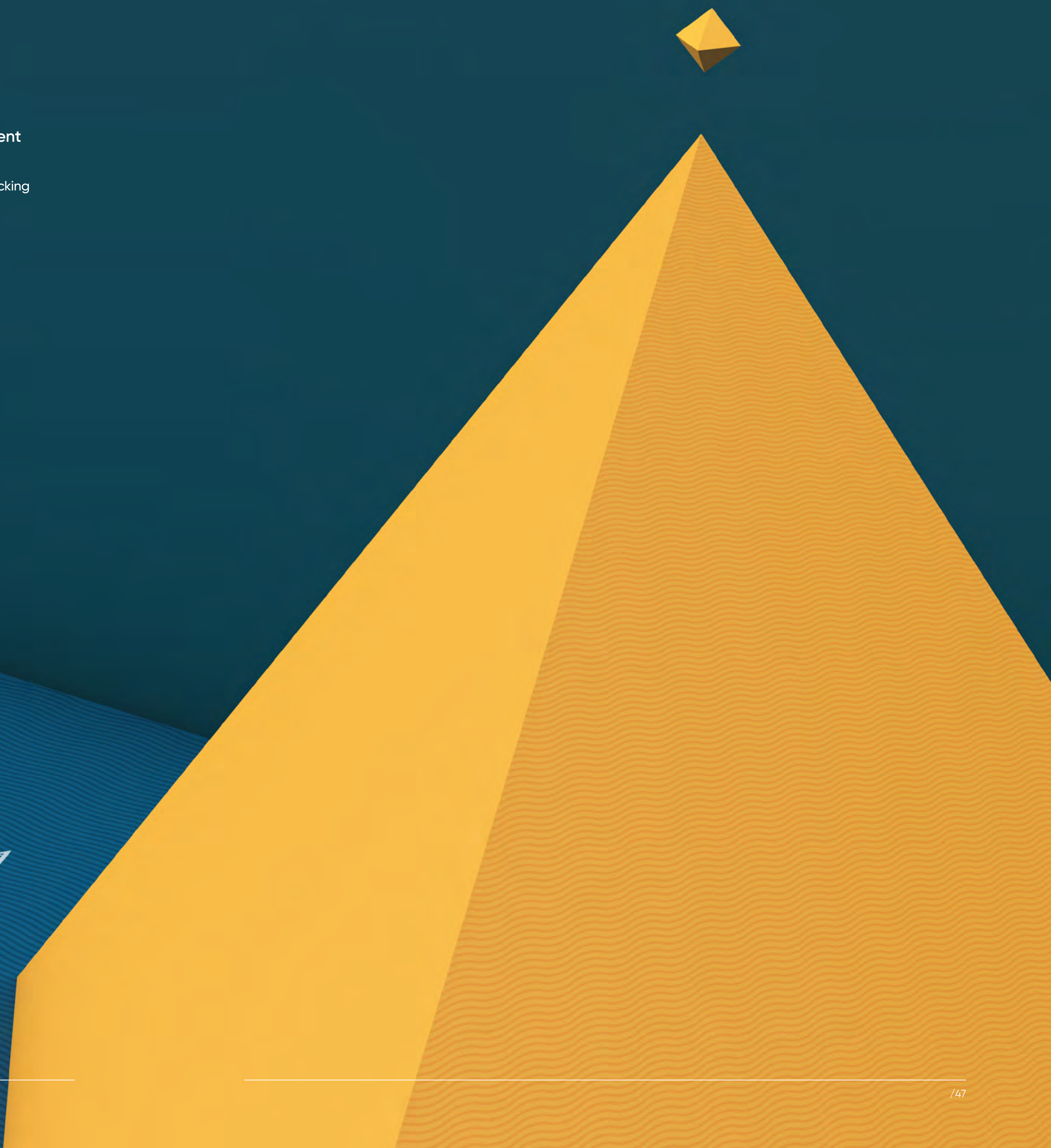
CONCLUSION

We are seeing sustainability becoming more central to managers' and investors' considerations. 2020 will be a crucial year for codifying and embedding the EU sustainable finance measures, along with similar initiatives emanating from the UK and other jurisdictions. The current investment landscape presents an opportunity to align operating, legal and governance approaches to ensure long-term value through sustainable business conduct. We expect in many cases this will involve re-examining portfolio company governance as voluntary frameworks develop into legal requirements.

MATTHEW BAKER
Partner,
London

CHRIS ORMOND
Associate Director,
London

FINANCIAL CRIME AND INVESTIGATIONS



BUILDING BRIDGES

ADDRESSING CHALLENGES IN CROSS-BORDER INVESTIGATIONS

The speed and co-ordination of enforcement authorities is ever increasing. As recently as October 2019, the US and UK signed an agreement under the US Cloud Act that allows each country to access data held in the other country pertaining to suspects in criminal investigations.

This will substantially reduce the time it takes for enforcement bodies in those countries to move forward on cross-border criminal investigations, including ones that focus on financial institutions involving sanctions, money laundering, market manipulation and anti-corruption.

Companies conducting cross-border internal investigations will therefore be under increasing pressure to conduct those investigations even more swiftly and efficiently. To do so, they must be prepared for and overcome the challenges presented by such cross-border investigations. Those challenges include dealing with multiple enforcers, data collection and review, appropriately interviewing employees and protecting attorney-client privilege. Below we briefly address those challenges.

DEALING WITH MULTIPLE ENFORCERS

A cross-border investigation will likely raise the interest of multiple enforcers. This affects the key decisions of whether to disclose an issue that you are investigating and, if so, to whom. Understanding the enforcement priorities of those jurisdictions, their past enforcement history, and your company's relationship to each jurisdiction is important to making the right choice as to whom to disclose. Further, you should have a clear idea of which jurisdiction you want to take the lead on any enforcement issues and try to guide all jurisdictions to agree with that choice. That does not mean you can ignore other jurisdictions that may want to be involved. It is essential to set up clear lines of communication with those other jurisdictions, emphasising that selecting a primary jurisdiction is important for efficiency and speed; and that all jurisdictions will receive the results of the investigation. Establishing a good relationship at the start can help mitigate multiple penalties in the end.

DATA COLLECTION AND REVIEW

One of the first steps taken in a global investigation is to collect relevant data and materials. When those exist in multiple countries, you must be aware of data protection legislation in each country. For example, it is fairly straightforward to collect and review data in the US, even personal data that is stored on a company computer. However, within the EU, the General Data Protection Regulation ("GDPR") restricts what companies can collect in terms of personal data and also restricts what data can be exported outside of the EU. It is critical that from the onset of the investigation, you should set out a document collection and review protocol that does not fall foul of data protection statutes.

> It is critical that from the onset of the investigation, you should set out a document collection and review protocol that does not fall foul of data protection statutes

INTERVIEWING EMPLOYEES

Your investigation will include interviews of employees in multiple jurisdictions, presenting a number of challenges – the first being language. Cultural sensitivities also should not be ignored. Each interview should comply with local labour laws. The purpose of these interviews is to gather factual information to determine what actually occurred and who are the culpable individuals, and then provide legal advice to the company. If individual witnesses are not forthcoming because of the interviewers' failure to employ best methods to obtain information, the investigation will inevitably suffer. This may in turn affect remedial actions the company considers taking; the company's credibility with enforcers when self-reporting; and the ability to obtain co-operation credit, where available.

PROTECTING ATTORNEY-CLIENT PRIVILEGE

Protecting attorney-client privilege to the maximum extent possible gives a company more flexibility in its handling of a global internal investigation. Even if a decision is made to disclose results to enforcers on a voluntary basis, it is important to protect core legal advice given to the company. To do so, the investigators must take steps from the beginning to create a record of material over which the privilege applies.

Key decisions include:

- Considering local laws protecting privilege
- Which country is liable to lead the enforcement
- Where company control of the investigation will rest
- Who will conduct the investigation
- The role of in-house counsel and where they are located
- How documents are collected and reviewed
- How witnesses will be interviewed
- How interviews will be memorialised.

Decisions on each of these issues will affect whether and to what extent attorney-client privilege will apply. There are very different expectations by enforcers in the US and the UK as to whether material over which privilege attaches should be provided, if co-operation resulting in a deferred prosecution agreement or declination is sought.

CONCLUSION

The challenges of a cross-border investigation are many and difficult. To ensure that your internal investigation is prepared to overcome those challenges, proper guidance and preparation are necessary, anticipating the multitude of legal and regulatory issues that arise in each of the relevant jurisdictions. Knowing what to expect and planning accordingly is critical.

MARK SRERE
Partner,
Washington DC

LAURA PERLOV
Partner,
Denver

NAOMI MILES
Senior Associate,
London

COLLECTIVE ACTION

UK COLLECTIVE CARTEL CLAIMS: AN EMERGING RISK CLASS

In recent years competition enforcement has pivoted from traditional industrial manufacturing sectors to the financial sector, bringing with it an increase in follow-on legal claims from aggrieved businesses and consumers. The new collective claims regime in the UK is an emerging risk for the financial sector, but the early settlement approach favoured in US class actions is not necessarily what fits the bill here.

Over the last decade, competition authorities around the world have pursued multiple investigations across the financial services sector and imposed billions of pounds of fines on banks and other firms. Several individuals have faced criminal prosecution.

Whilst the US authorities initially led this charge, enforcement activity in Europe has included:

- A European Commission investigation into anti-competitive behaviour in foreign exchange ("FX") spot trading, which led to fines of a combined total of €1.07 billion in May 2019
- The Commission's imposition of fines totalling €1.3 billion for manipulating the Euribor benchmark
- The imposition by the FCA of its first competition law fine, in the asset management sector, in February 2019
- Ongoing investigations in the bonds sector (by both the Commission and the UK's Competition and Markets Authority), the aviation insurance sector (by the Commission) and FX (by the Commission).

Most financial services firms have long been aware that this change in focus for the authorities, away from the industrial and manufacturing sectors, has created a significant new compliance risk. What is now emerging, as a result of this increased public enforcement drive, is a concurrent increase in legal claims from organisations and individuals that have allegedly suffered loss as a result of the anti-competitive conduct.

In 2015, the UK introduced a collective actions procedure which allowed for US-style "opt out" class actions to the English courts, making it easier for claimants with lower value claims, including end consumers, to pursue claims. EU-wide procedures remain under consideration.

Of the five collective actions that have so far been filed in the UK, two have concerned the financial sector – a collective action seeking £14 billion in damages against Mastercard in relation to interchange fees, and a claim against five banking groups in relation to FX manipulation estimated to be worth up to £6 billion. Both claims are at an early stage, with the UK's Competition Appeal Tribunal yet to determine whether those claims should proceed beyond the initial class certification stage.

EUROPEAN COMMISSION FINES

€1.07bn – FX anti-competitive behaviour

€1.3bn – Euribor benchmark manipulation

COLLECTIVE ACTIONS FILED IN THE UK

€14bn – Mastercard interchange fees

€6bn – FX manipulation claimed against 5 banking groups

Those cases lag well behind the equivalent cases in the US, where in 2018 the FX and interchange fee class actions settled for approximately $2.3 billion and $6 billion respectively. However, those earlier stage settlements reflect the fact that class actions have existed in the US for decades and the "big issue" legal principles have long since been resolved.

The biggest unresolved issue in the UK collective actions regime is the extent to which damages claimed on behalf of a class must represent an accurate measure of each individual claimant's losses. This reflects English law principles that any damages awarded in litigation must be purely compensatory, whilst under US law punitive damages are available.

This has been the key issue in the collective action against Mastercard. That claim was initially dismissed by the Tribunal as the claimants struggled to calculate losses on behalf of the class.

However, following a successful appeal it has been remitted to the Tribunal for further consideration. Whilst settlements have been secured in a LIBOR class action in the US, LIBOR-related claims have proved difficult for claimants to quantify even on an individual claim basis in the UK. Similar issues are likely to arise in the FX collective action. As long as fundamental questions such as this remain unanswered, defendants may be less inclined to settle collective actions brought in the UK.

CONCLUSION

Given the global nature of the financial services industry, financial institutions that have been found to have engaged in anti-competitive behaviour are likely to face lawsuits in multiple jurisdictions from those claiming to have suffered loss. Local solutions may be most effective for this global problem – whilst early settlement of US class actions may be the wisest move, the smart money is, for now, on fighting the collective actions in the UK.

SARAH WARD
Associate Director,
London

ANDREW LEITCH
Associate,
London

PUT TO THE TEST

WHAT IS THE FCA LOOKING FOR FROM FIRMS' APPROACH TO FINANCIAL CRIME PREVENTION?

The FCA's Enforcement division currently has around 90 financial crime investigations, which represents 13% of its total number of investigations. This is a significant increase from four years ago when there were just 12 financial crime investigations, representing 5% of open investigations. What is the FCA looking for?

In testing whether financial crime risks are properly managed by firms, whether from an enforcement investigation perspective or at a supervisory deep dive visit, the FCA adopts a similar approach in reviewing firms' financial crime systems and controls. Across a range of suspected regulatory breaches – from market abuse surveillance controls, to anti-money laundering controls, and in conducting supervisory visits to understand controls around anti-bribery and corruption – the FCA's model tests a number of core themes, five of which are discussed below.

FCA's Enforcement division financial crime investigations

2015	12	5%	of total investigations
2019	90	13%	of total investigations

FCA open investigations into culture

2015	0
2019	70

1. CULTURE AND GOVERNANCE

One key new approach is the testing of a firm's approach to culture and governance. We see this focus reflected in the fact that there are currently around 70 open investigations into culture (compared with none just four years ago). In testing culture and governance, the FCA wants to understand how the board manages financial crime risk and provides oversight. Questioning in this area will include a focus on the quality and categories of management information provided to the board.

The FCA may look to test:

- How the management information is selected – has the board specifically requested categories of data in order that it can manage risk, or is it reliant on whatever the head of a function chooses to escalate?
- Are there examples of how the board takes decisions in relation to the data it is given?
- How are decisions taken by the board cascaded down into the business?

2. BOARD UNDERSTANDING

An important area of focus for the FCA is in relation to the board's level of understanding of the underlying issues it is required to manage.

- Sometimes board committees managing financial crime risks do not receive training on how financial crime may take place. This can lead to questioning from the FCA on how the board can properly manage and understand risks if they have not been properly trained on what the relevant financial crime is.

3. DEVELOPMENT OF CONTROLS

In looking at a firm's controls, the FCA will first look to understand how the controls were developed. The risk assessment documentation will be the FCA's starting point and the regulator will want to understand how a firm has gone about understanding where the risks of financial crimes arise across its businesses. The FCA then seeks to understand how the controls have been developed in order to mitigate against the risks identified.

- It may look fantastic to have an intricate set of policies in place – but if they do not properly address the risks faced by the businesses of the firm, or if they are academic and just say what the law is, the FCA is likely to question whether anyone actually understands what they mean and whether they are properly tailored. Showing how controls are tailored and thoughtfully produced by reference to the risks identified will be important to convey.

4. RESOURCING

Where a firm can demonstrate that it has an extensive set of documents listing controls, unless it demonstrates that the controls work and are implemented, the FCA is unlikely to take much comfort from the documents.

- Having a set of documented controls in place which are not operating appropriately is more likely to lead the regulator to conclude that there is a resourcing problem and that the management of financial crime risks is not being sufficiently prioritised by the firm. The FCA looks to see how firms monitor and check that the control framework actually works.

5. ASSURANCE AND REVIEWS

In assessing the effective operation of controls, the FCA looks to understand how quality assurance takes place and whether decisions taken by Compliance staff (for example in relation to closing alerts) are correctly made and sample-checked.

As the risks that firms face are constantly evolving, the FCA will be testing to understand the triggers for the development of new controls and the process by which existing controls are reviewed.

- Where a new regulatory change is introduced, the FCA will look to see if a gap analysis has been conducted and how the firm goes about deciding if new policies or procedures need to be introduced.

CONCLUSION

In managing financial crime risks, the FCA's methodology of the assessment of controls is likely to continue to focus on these core themes. Reviewing and assessing financial crime control frameworks, particularly in relation to anti-bribery and corruption, is likely to remain a key area of focus for the FCA in 2020.

ANDREW TUSON
Partner,
London

THE LONG ARM OF OFAC

NON-US ENTITIES SHOULD STILL BE MINDFUL OF THE REACH OF US SANCTIONS

Corporates based outside the US continue to find themselves targets of US sanctions enforcement actions, with significant consequences attaching. Financial institutions continue to be a focus of enforcement efforts; in the last three years, there have been 14 US sanctions enforcement actions relating to financial services, making it the most prevalent industry among settlements published by the US Office of Foreign Assets Control ("OFAC"). Of the 2019 settlements with OFAC, the two highest settlement amounts by early December were against non-US financial institutions – each resulted in financial penalties of over $600 million.

Despite most aspects of US sanctions programmes focusing on US persons (i.e., US citizens, permanent residents, anyone physically located in the United States, and companies organised under the laws of a state or territory within the United States), all programmes have provisions that make it a violation for anyone (US or non-US) to avoid or evade the sanctions, as well as to cause another party to violate the sanctions. Moreover, the US sanctions against Cuba and Iran require non-US subsidiaries of US persons to comply with all aspects of those sanctions programmes.

2017–19

14 US sanctions enforcement actions relating to financial services

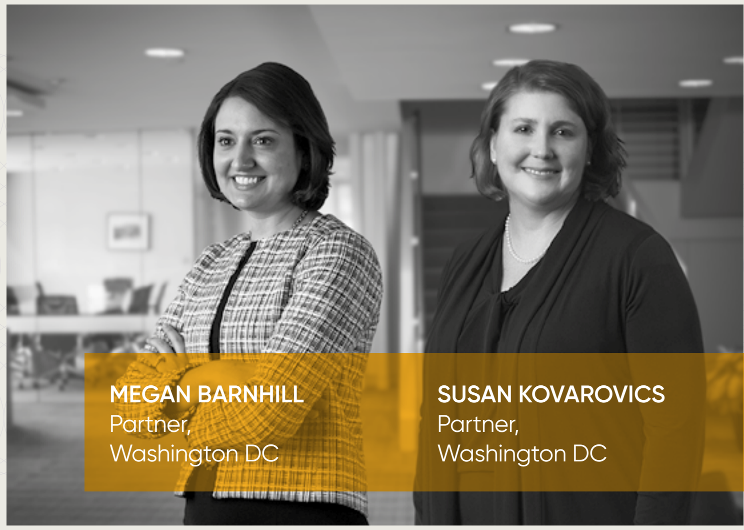
Failure to provide full information about transactions or to address red flags in transactions are among the common themes in these recent OFAC enforcement cases. For financial institutions, this included not disclosing the involvement of sanctioned parties or links to sanctioned destinations for transactions that were ultimately processed to or through the United States.

OFAC's wide reach for enforcement of US sanctions makes it critical that all financial institutions, wherever they are based, address risks under US sanctions as part of their sanctions compliance programmes.

This includes:

- Monitoring risks that could be triggered by engaging in transactions with destinations or parties targeted by US sanctions
- Ensuring transparency in all transactions, including by providing information regarding any sanctioned persons or destinations involved in the transaction to intermediaries
- Carefully considering the relevance of US sanctions for any transaction that may have a US nexus, even if your entity is not a US person. A US nexus may include, for example, transactions that will be processed to or through a US financial institution or its non-US branch.

Attention is also warranted to US secondary sanctions, which target foreign persons engaging in activities that may otherwise have no US jurisdictional connection. Taking actions contrary to US secondary sanctions will not result in a violation or imposition of a penalty pursuant to an enforcement action. However, such actions can result in an entity being prohibited from opening or maintaining correspondent or payable through accounts in the United States or being named as a Specially Designated National. Such an outcome may well be much more costly than a financial penalty, as SDN status will severely curtail your pool of clients and business partners. Addressing these secondary sanctions risks in sanctions compliance programmes is therefore also very important.



MEGAN BARNHILL
Partner,
Washington DC

SUSAN KOVAROVICS
Partner,
Washington DC

THE CHANGING LANDSCAPE OF TAX RISK

REAL-TIME ENGAGEMENT WITH HMRC

The UK tax landscape is characterised by heightened tax regulatory obligations, with more than 100 measures introduced by government over the last decade to regulate tax non-compliance. In the year ahead, there are a number of key considerations that firms will need to keep in mind when dealing with HMRC.

Key findings from a survey that we recently undertook of senior tax professionals in financial services and other industries provide a fascinating insight into the tax risk issues that UK firms face:

- Firms are concerned about the increasingly interventionist approach of HMRC, with 67% of respondents saying the increase in tax regulation has a significant impact on their businesses. For financial services firms, the corporate criminal offence for the failure to prevent the facilitation of tax evasion has resulted in an increased compliance burden
- Half of respondents said the number of HMRC enquiries has increased over the past few years, relating to a wide range of taxes, particularly corporation tax, VAT and transfer pricing
- While the relationships between firms and their HMRC relationship manager (known as a "CCM") is generally positive, a common theme is that CCMs have their limitations as they do not have sufficient authority to make decisions. This can frustrate resolution of disputes
- Delay on the part of HMRC is a significant issue facing firms involved in tax disputes. This has also been identified as a major problem by the House of Lords Economic Affairs Committee, with the balance of power tipping too far in favour of HMRC.

Where disputes with HMRC arise, financial services firms should be particularly mindful that:

(1) HMRC appears to have an increasing appetite to pursue enquiries into financial services firms in respect of transfer pricing and diverted profits tax. Given the complexity of such disputes, such enquiries are likely to be protracted unless firms maintain pressure on HMRC to accelerate resolution

(2) The government has set HMRC a target of collecting an additional £2 billion by 2023/24 from tax non-compliance. This means achieving settlements with HMRC is likely to remain difficult.

In the current climate, prevention is therefore better than cure and firms are advised to seek to minimise the risk of tax disputes arising, in particular through strong controls and real-time engagement with HMRC.

> The government has set HMRC a target of collecting an additional £2 billion by 2023/24 from tax non-compliance

100+

New measures against tax non-compliance since 2010/11

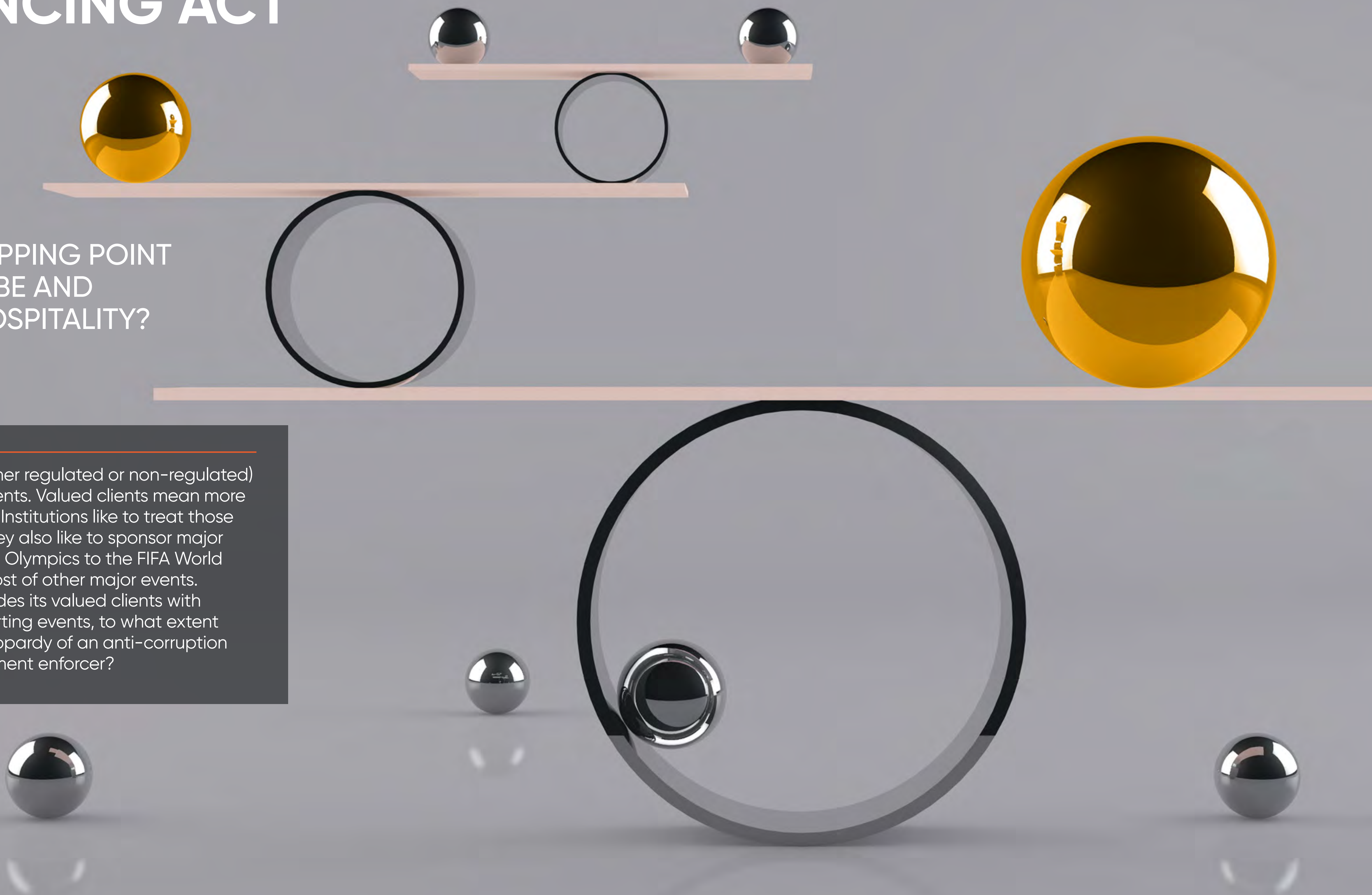
67%

Of firms say the increase in tax regulation has a significant impact on their businesses

KATE ISON
Partner,
London

JESSICA HOCKING
Associate,
London

A BALANCING ACT



WHERE'S THE TIPPING POINT BETWEEN A BRIBE AND CORPORATE HOSPITALITY?

All large corporates (whether regulated or non-regulated) have their most valued clients. Valued clients mean more business and more profits. Institutions like to treat those valued clients well. And they also like to sponsor major sporting events – from the Olympics to the FIFA World Cup to Wimbledon to a host of other major events. When the corporate provides its valued clients with tickets to those major sporting events, to what extent will it be putting itself in jeopardy of an anti-corruption investigation by a government enforcer?

With the Tokyo Olympics just around the corner, corporates should ensure that they do not inadvertently run afoul of anti-corruption laws when they provide hospitality to their clients in connection with such major sporting events.

This issue is certainly on the radar screen of US enforcers – perhaps more so than many firms realise. In May 2019, the US SEC extracted more than $4 million from Telefônica Brasil for the way it handed out tickets and hospitality to the 2014 World Cup and the 2013 Confederations Cup.

$25m US SEC fine to BHP Billiton for 2008 Beijing Olympics hospitality

176 invited officials

$500k World Cup tickets

93 government officials

$4m US SEC fine to Telefônica Brasil for 2014 World Cup and 2013 Confederations Cup hospitality

$100k Confederations Cup tickets

34 government officials

Before that, in 2015 the SEC fined BHP Billiton $25 million for its hospitality programme associated with the 2008 Beijing Olympics. In each case, relying on the US Foreign Corrupt Practices Act's ("FCPA") prohibition of bribing "foreign officials", the US government focused on the company's lack of internal controls to ensure that such hospitality was not used to provide incentives for "foreign officials" to conduct business with the company.

In the Telefônica case, the company gave more than $500,000 worth of World Cup tickets and related hospitality to 93 government officials and more than $100,000 worth of Confederations Cup tickets and hospitality to 34 officials. In the Billiton case, the company invited 176 government officials and 60 attended. The nature of the hospitality was also important. In many cases spouses were invited and business class air fare included. For the Beijing Olympics, the total excursion package (without air fare) was valued between $12,000 to $16,000 per person, and included sightseeing tours and luxury hotel accommodation.

The UK Serious Fraud Office has not brought any prosecutions of this nature to date. However, because the scope of the Bribery Act is much broader than the US FCPA – its prohibitions include purely commercial bribery not involving foreign officials – the SFO could well jump on the enforcement bandwagon with respect to this issue.

The UK Ministry of Justice addressed the specific issue of corporate hospitality, in its Bribery Act 2010 Guidance issued shortly after the enactment of the UK Bribery Act (as the UK was preparing for the 2012 London Olympics). According to the Ministry:

"Bona fide hospitality and promotional, or other business expenditure which seeks to improve the image of a commercial organisation, better to present products and services, or establish cordial relations, is recognised as an established and important part of doing business and it is not the intention of the Act to criminalise such behaviour."

It appears from this that there may be more leeway in the UK's attitude toward corporate hospitality than the attitude demonstrated in the US. However, it remains a grey area and one in which corporates frequently seek advice.

Yet under both regimes, a corporate should be prepared to demonstrate that its use of expensive hospitality was not done in violation of applicable anti-corruption laws. The best way to do so is for the corporate to set up a specific procedure that will govern all hospitality related to the event. Compliance and legal can then ensure that the hospitality will not violate various anti-corruption laws and the corporate's own anti-corruption policy and procedures. In the context of these premium sporting events we recommend that the corporate creates specific compliance procedures before making corporate hospitality available for the event, which include:

- Compliance and legal personnel involvement in the approval process of all hospitality for the event
- Appropriate training for those giving the offers and those reviewing and approving the offers
- Identification of risks involved in inviting "foreign officials"
- Determination of whether the institution has any pending business with each potential invitee (not only at the time of the invitation, but also at the time of the event)
- Ability to update information in the approval process where business circumstances evolve
- Review of the proportionality of the hospitality
- Proper accounting of the hospitality.

CONCLUSION

Premium sporting events can be great client relationship building events. Corporate hospitality is not prohibited. Yet that hospitality must be reviewed in the context of the US FCPA and the UK Bribery Act. Establishing bespoke internal procedures for each such event that follow the above guidelines should help institutions steer clear of potential government investigation.

MUKUL CHAWLA QC
Partner,
London

JENNIFER MAMMEN
Counsel,
Washington DC

FIGHT THEM ON THE BREACHES

DATA BREACH CLASS LITIGATION GAINS MOMENTUM – IS THERE A BETTER WAY TO MANAGE IT?

In this publication last year we flagged the possibility of more group or class litigation following a data breach. Recent Court decisions have confirmed that this is indeed the direction of travel for significant data breaches in the UK.

But should financial institutions now be considering whether there could be a better way to manage these group claims, perhaps through the collective redress schemes that have worked well for compensating losses caused by mis-selling?

Recent Court decisions have clarified two key points that were previously seen as barriers to successful group actions in the UK – the concept of what "damage" is caused by a data breach, and the difficulties in obtaining a Group Litigation Order for class litigation.

In *Lloyd v Google* the Court of Appeal reversed the lower court's decision and ruled that a loss of control of personal data was "damage" of itself, and that this damage could be compensated financially without the need for the claimant to show any actual financial loss or distress. This moves away from the previous position that a claimant needed to identify actual financial harm or distress as a precursor to a monetary award.

This approach also overcame another common difficulty in progressing representative claims – proving that all members of the class have the "same interest" in the claim. The Court felt that all claimants had suffered the same loss of control of their data. The lead claimant gave up any reliance on the individual circumstances of claimants, effectively bringing damages to the lowest common denominator.

However, this was only a preliminary decision in the context of seeking permission to serve the claim abroad. It remains to be seen whether the claim will succeed and what quantum of damages, if any, will be awarded.

Moreover, claimants will still need to prove the claim has passed the de minimis threshold of being "non-trivial". Financial institutions may find some comfort in Sir Geoffrey Vos's obiter comment: "that threshold [of seriousness] would undoubtedly exclude, for example, a claim for damages for an accidental one-off data breach that was quickly remedied."

In a second recent case, *Weaver*, the High Court has approved a Group Litigation Order for claims against British Airways for data breaches in 2018.

An interesting feature of the British Airways Group Litigation Order is the test set out for inclusion in the "class": to join the action an individual must have been notified by British Airways of the data breach, must raise an issue of whether British Airways is liable to that individual for damage, and the individual must have suffered damage (which is not limited to financial loss or distress). It seems that the concept of damage for data breaches is one that will continue to be the focus of these initial UK litigations for now.

> The true cost of a data breach to a financial institution could be significantly more than the €20 million/4% global turnover figure that has been much publicised under the General Data Protection Regulation

Together, these two decisions appear to move the UK closer to a culture of collective actions for data breach litigation. This leaves financial institutions subject to potentially significant liabilities for data breaches affecting large numbers of users. Combined with exposure to the Information Commissioner's Office, the financial regulators and now potential class litigants, the true cost of a data breach to a financial institution could be significantly more than the €20 million/4% global turnover figure that has been much publicised under the General Data Protection Regulation.

As an alternative to class litigation, firms may be better served by offering voluntary collective redress. While collective redress schemes are fairly common in financial services, they have been less common to date in respect of data breaches. News International offered a collective redress scheme in the phone-hacking scandal but victims were reluctant to enter it in preference to court claims as there was no tariff for damages suffered for this relatively new sort of claim. It remains to be seen whether this alternative proves attractive to victims of data breaches.

CONCLUSION

Where there has been a breach, firms will need to distinguish between meritorious claims from impacted data subjects and vexatious litigants who are easily mobilised by consumer groups. A voluntary collective redress scheme, or one imposed by regulators, may help firms do that on a more cost-effective basis whilst also appearing public and regulatory criticism.

ORAN GELB
Partner,
London

SARAH MCATOMINEY
Senior Associate,
London

JACK DUNN
Trainee Solicitor,
London

DIGITAL

CLARIFYING THE CRYPTIC

CLEAR AND SENSIBLE REGULATION IS VITAL TO BLOCKCHAIN'S SUCCESS IN FINANCIAL SERVICES

Blockchain technology has the potential to disrupt traditional business models across all sectors of the economy, particularly in financial services. The technology's rapid evolution presents both opportunities and risks. To maximise its positive impact, a clear, business-friendly legal and regulatory framework is essential.

Across the world the regulatory treatment of blockchain technology remains diverse. Within the EU, member states often take different approaches but the EU is slowly developing EU-wide frameworks such as the European Securities and Markets Authority's ("ESMA") recent advisory on initial coin offerings and cryptoassets. Regulatory oversight within the US is likewise divided across multiple federal and state regulators. We briefly consider the regulatory approaches in three key jurisdictions.

UNITED STATES

Much of the recent regulatory activity in the US has come from the Securities and Exchange Commission ("SEC"), Commodities Futures Trading Commission ("CFTC"), Financial Crimes Enforcement Network ("FinCEN") and Internal Revenue Service ("IRS"). In April 2019, the SEC released a statement on "Framework for 'Investment Contract' Analysis of Digital Assets" to help market participants determine whether a digital asset is a security, both at issuance and later.

In July 2019, as part of market discussions to develop ways to establish possession or control by broker dealers over their customers' digital asset securities, the SEC and the Financial Industry Regulatory Authority ("FINRA") issued a joint statement identifying scenarios that avoid custody concerns altogether. For example, where broker dealers do not act as intermediaries or take possession of the digital asset securities.

In October 2019, CFTC Chairman Tarbert clarified in public remarks that he considers both Bitcoin and Ether to be commodities (and not securities). In the same month, the IRS released guidance addressing taxation of digital assets and virtual currencies, including appropriate calculation of gains and losses. And the SEC continues to police fraud and unregistered offerings in the digital asset context.

Regarding money transmission and anti-money laundering concerns, in May 2019, FinCEN issued guidance on convertible virtual currencies detailing how:

(1) Money transmission regulations apply to common business models involving convertible virtual currencies

(2) Financial institutions can identify and report suspicious activity relating to convertible virtual currencies.

On 11 October 2019, FinCEN, the SEC, and CFTC issued a joint statement highlighting anti-money laundering and counter-terrorism obligations in the digital asset space.

Importantly, blockchain when used as a medium of exchange, for example Bitcoin, is not currently regulated in the UK. This may, however, change in the coming months following various public enquiries on the subject

UNITED KINGDOM

The regulatory approach to blockchain in the UK is essentially based on a functional characterisation of how blockchain is being used in a particular situation. On this basis, many applications of blockchain fall within the existing regulatory framework. For example, tokens that are properly characterised as securities (as opposed to pure utility tokens) are regulated investment products. Therefore issuing them could potentially be subject to the prospectus requirements and providing certain services in connection with their issuance and secondary market trading are very likely to require the service provider to be licensed.

Importantly, blockchain when used as a medium of exchange, for example Bitcoin, is not currently regulated in the UK. This may, however, change in the coming months following various public enquiries on the subject. In contrast, derivatives over cryptocurrencies are regulated financial products.

Notably in November 2019, the LawTech Delivery Panel published a Legal Statement on Cryptoassets and Smart Contracts. This document concludes that, under existing English law, most cryptoassets are capable of being legal property and smart contracts are capable of satisfying the basic requirements for a legal contract. This may well help to reduce much of the legal uncertainty relating to cryptoassets and smart contracts and thereby make the UK a more attractive place to do blockchain-based financial services business.

GERMANY

Like the UK, Germany aims to be the EU front runner for setting a comprehensive regulatory framework for blockchain technology, proposing not only an overall blockchain strategy but also the enactment of new regulatory authorisation requirements.

Draft legislation has been prepared which will implement new licensing requirements for operators of electronic wallets storing the client's key(s) and bring certain tokenised services to customers within the scope of regulation in Germany. When the new law comes into force, the provision of brokerage and exchange services in currency tokens, securities tokens, and certain other tokens (most likely excluding utility tokens) will trigger the need for a banking license. As these activities will be regulated services, anti-money laundering requirements will also apply.

CONCLUSION

Although 2019 saw a number of tangible developments in legal and regulatory approaches to blockchain technology, the sphere remains in its infancy. 2020 will see additional legal and regulatory initiatives; the emergence of recognisable trends in the application of existing rules; and further sophistication in interactions between market participants and regulators.

DANIEL CSEFALVAY
Partner,
London

BERND GEIER
Partner,
Frankfurt

BEN SAUL
Partner,
Washington DC

MEET THE BODYGUARD

THE NEW STANDARD FOR PAYMENT SECURITY IS ON ITS WAY, WITH SCA

The new strong customer authentication ("SCA") requirements under the EU Payment Services Directive ("PSD2") went live on 14 September 2019. While the new requirements apply only to payment service providers such as banks and non-bank payment processors, and are subject to an initial "no enforcement" period in certain EU member states, their implications will be felt over the coming year by regulated and non-regulated businesses throughout the payment processing chain.

WHAT IS SCA?

In summary, SCA is a process whereby a payment service provider authenticates a customer's identity by using at least two elements from three specified categories:

- Knowledge – something only the customer knows (such as a password)
- Possession – something only the customer has (for example a token generator)
- Inherence – something the customer is (essentially, biometrics such as fingerprints).

Knowing one element must not compromise the other, and each of the two elements must come from a different category.

For remote electronic payments, such as online payments, the transaction must also be dynamically linked to a specific amount and a specific payee (for example via a one-time passcode).

WHEN MUST SCA BE APPLIED?

SCA must be applied when a customer:

- Accesses their payment account online
- Initiates an electronic payment, or
- Carries out any action through a remote channel that may imply fraud,

in each case, unless an exclusion/exemption is available.

It is always the payer's payment service provider (e.g. a card issuer) that determines whether to apply SCA or use any exemption. However, the payee's payment service provider (such as a merchant acquirer) can decide on certain exemptions (subject to the issuer's final decision).

WHAT IS THE POTENTIAL IMPACT?

The new requirements are different from most of the existing two-factor authentication methods – for example, a password and a PIN will not constitute SCA, because both are "knowledge" elements. This means that changes may need to be made to the existing processes. For example, the major card schemes (Visa, Mastercard and Amex) are deploying 3D Secure Version 2 across the EU card payment market.

Regulated payment service providers are directly impacted. Non-regulated businesses (such as merchants) may also need to implement changes as required by their payment service providers so that the payment service providers themselves can comply. In certain circumstances, merchants can be liable for SCA failures.

WHAT ARE THE EXCLUSIONS/ EXEMPTIONS?

Payments initiated by a payee such as a merchant (known as "merchant initiated transactions" or "MIT") are excluded. This includes utilities payments (typically through direct debit) and certain subscription services. However, the initial set-up of the MIT mandate may require SCA.

There are nine exempted situations where SCA is not required:

(1) Accessing accounts within 90 days (rolling) to check balances and transactions, provided that no sensitive payment data (such as a password) is disclosed

(2) Contactless payments not exceeding €50 (individually) where either the number of consecutive transactions does not exceed five or the cumulative value does not exceed €150

(3) Payments made at unattended terminals for transport fares or parking fees

(4) Payments made to trusted beneficiaries that the customer set up in advance with their account payment service provider

(5) Recurring payments to the same payee with the same amount (such as a standing order)

THE THREE ELEMENTS

(6) Credit transfers between one's own accounts with the same payment service provider

(7) Remote payments not exceeding €30 (individually), where either the number of consecutive transactions does not exceed five or the cumulative value does not exceed €100

(8) Corporate payments through dedicated processes (subject to regulatory approval)

(9) Remote payments where the payment service provider's overall fraud rate is within specified thresholds.

The timing and other thresholds above are calculated by reference to the last time SCA was applied.

> "Full SCA compliance is expected by 14 March 2021 in the UK"

WHAT IS THE CURRENT STATUS?

Given the potentially significant impact, the European Banking Authority ("EBA") opined in June last year that member states might have a no-enforcement period for online card payments. As a result, while the rules formally applied from 14 September 2019, national regulators may choose not to enforce them during a short period. The Financial Conduct Authority announced in August an 18-month no-enforcement period; full SCA compliance is therefore expected by 14 March 2021 in the UK. Subsequently, the EBA further opined in October that compliance should be completed by 31 December 2020 for all member states. So far, there have been no indications that the FCA will change the UK position.

CONCLUSION

Application of SCA is currently fluid across the EU. In the UK, online payments should be "business as usual" for now, but changes are expected to be gradually implemented to meet the new deadline. However, certain in-store payments may require immediate changes.

Frictions may arise for cross-border payments given the inconsistency between the UK position and the EBA approach which, although expected to be followed by other member states, may be adopted with local differences.

KAI ZHANG
Associate Director, London

PREDICTIVE TECH

NEXT-GEN AI IS HELPING COMPLIANCE MONITOR ROGUE OPERATIONS

Financial institutions are now very familiar with automated surveillance systems designed to monitor the behaviour and communications of their staff and identify instances of suspected market abuse or other misconduct at work. The threat of large fines and criminal prosecution may deter some rogues, but those seeking to operate below the radar will always find more creative ways to operate.

This presents a challenge for firms, but new technology may be the answer. Employee surveillance has already seen significant advances with the widespread use of communication monitoring tools to flag particular keywords and phrases and the application of pre-specified scenarios to reveal specific types of misconduct – but what if it were possible to get into the minds of how employees operate?

A new generation of artificial intelligence ("AI") and machine learning technologies utilises communications data to predict the behaviour of employees and flag rogue operations in real time. These advances can greatly benefit financial services compliance teams, as firms harness the very real value that these technologies can deliver in identifying problematic conduct at an early stage.

An employee's behavioural changes can now be identified through AI and machine learning, analysing an individual's communications to identify patterns and develop a smart algorithm. This goes beyond direct matching for specific content, which can often result in compliance teams being impeded by numerous "false positive" results. AI is able to detect the tone of an inappropriate or suspicious communication, and other subtle signals such as the time of day a communication is sent.

Data models and "profiles" about the behaviour of a trader are developed. As the trader alters their communication style the profiles reflect this, continuously learning in real time. In turn, monitoring rules and triggers can be updated, allowing the AI to proactively flag "smoking gun" communications as they occur, and enabling legal and compliance teams to identify issues and take protective actions before an issue escalates.

Our forensic technology team is seeing the deployment of complex AI technologies becoming more prominent in the financial services industry and across other sectors. These tools are also starting to be incorporated into document review platforms, which have always contained a level of built-in analytics. The technology is being used for discovery and unstructured data investigations, leading to quicker responses and significantly lower costs in locating any problematic conduct.

The technology is developing so rapidly that internal stakeholders should be having regular conversations about the latest use of AI technology and trialling what is available in order to streamline surveillance activities and make them more effective.

> Those seeking to operate below the radar will always find more creative ways to operate

JASON ALVARES
Forensic Technology Manager,
London

SIÂN COWAN
Associate,
London

FRIEND OR FOE?

IS REGULATORY CHANGE A THREAT OR A CATALYST FOR BUSINESS IMPROVEMENT?

Faced with the rising tide of new law and regulation both domestically and internationally, legal and compliance teams have the challenge of how best to implement changes in a manner that supports rather than undermines the business that they support.

Many of our clients are now viewing the implementation of new laws and regulations not simply as an additional obligation, but instead as an ideal opportunity to drive wider business improvement and deliver greater value to their organisations.

If a change programme is broadened to incorporate a process improvement initiative, there is the opportunity to offset the cost of new regulation by increasing efficiency, improving client satisfaction and driving wider strategic objectives.

Regulators are also mandating increasingly specific processes for compliance, so process re-engineering exercises are likely to become necessary in any instance.

We see the following five-stage approach as a key to success in achieving these two objectives:

- Scoping – understand the risk/complexity of regulatory change to engage impacted areas of the organisation
- Wider impact assessment – visualise the end-to-end process and understand downstream impacts on other processes/teams
- Process improvement workshops – identify changes to address new regulations as well as pain points and/or inefficiencies
- Outcomes assessment – measure anticipated benefits/cost savings which mitigate the cost of regulatory implementation
- Transformation roll-out – project-manage changes.

In order to achieve the highest levels of success, experts in process and project management who understand the legal landscape should be engaged. Buy-in from the board will also be essential, but increasing efficiency should naturally align with strategic business objectives.

In-house legal and compliance teams are increasingly leveraging legal and regulatory change to maximise business performance at the same time. Benefits include:

- Business engagement with regulatory change
- Robust compliance measurement and processes "baked in" to the organisation (rather than layered on top), providing hard evidence for regulators
- Cost savings and efficiency improvements that will, in many cases, outweigh the costs of regulatory compliance.

SUSAN WHITLA
Head of Process Improvement, London

NICK PRYOR
Regional Innovation Solutions Director, London

GLOBAL CAPABILITIES, LOCAL EXPERTISE.

1400 lawyers in 31 offices advising businesses across North America, Europe, the Middle East and Asia.

8x winner of the Law Firm of the Year award in different markets since 2004.

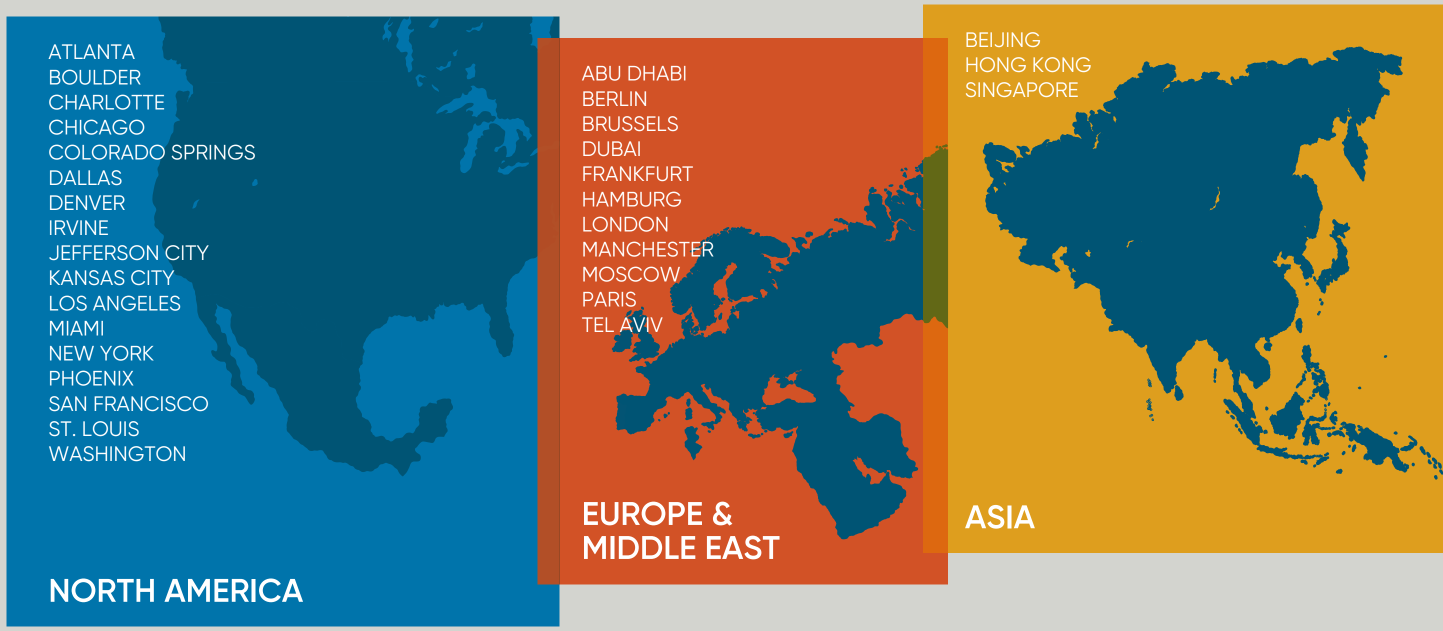
30 of the world's top 50 banks have relied on us.

40% of the Fortune 500 rely on our firm to support their business goals and protect their interests.

4x recent winners for legal innovation.

- **Most Innovative Law Firms for Business of Law; and**
- **Data, Knowledge & Intelligence: Managing & Developing Talent** (FT North America Innovative Lawyers 2018)
- **AI Innovation Award** (Legal Week Innovation Awards 2019)
- **Legal Services Procurement Innovation** (Legal Week Innovation Awards 2019)

WORKING FROM 31 OFFICES AROUND THE WORLD, OUR ADVICE HAS TOUCHED COUNTRIES THROUGHOUT THE AMERICAS, ASIA, EUROPE, THE MIDDLE EAST AND AFRICA.



Getting in touch
When you need a practical legal solution for your next business opportunity or challenge, please get in touch.

London
Adelaide House, London Bridge, London,
EC4R 9HA, England

bclplaw.com

Nathan Willmott
nathan.willmott@bclplaw.com
Tel: +44 (0)20 3400 4367

Mark Srere
mark.srere@bclplaw.com
Tel: +1 202 508 6050