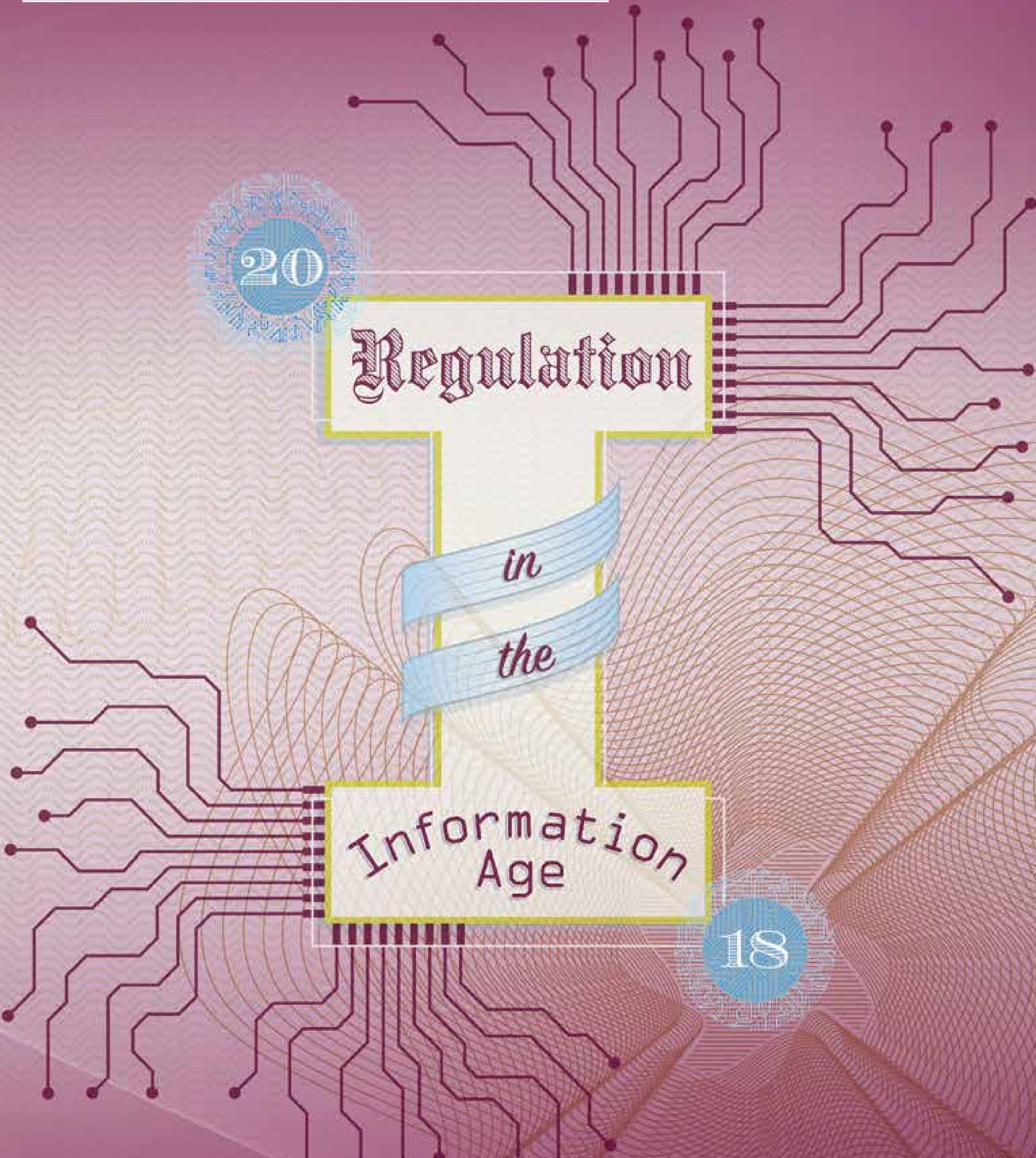
FINANCIAL REGULATION EMERGING THEMES IN 2018



FEATURED CONTENT

BERWIN LEIGHTON PAISNER

REGULATION IN THE INFORMATION AGE

Welcome to BLP's Emerging Themes 2018, in which members of our financial regulation group provide their own personal viewpoints on new and developing issues that will be impacting our clients over the year ahead.

Yet again we face the new year in the knowledge that there is huge change ahead. Having grappled with the uncertainties of MiFID II implementation to meet the January 2018 deadline, other major regulatory change projects continue in areas such as the General Data Protection Regulation, the Insurance Distribution Directive, the expansion of the Senior Managers and Certification Regime to all UK authorised firms, the ring-fencing of UK banks and, of course, vital restructuring of cross-border operations to enable continuity of services following the UK's secession from the European Union early next year.

The title we have chosen for this year's publication, "Regulation in the Information Age", reflects the key importance to many of the businesses that we advise of managing – and generating commercial advantage from – huge data flows, and the attempts of our national and European authorities both to seek to regulate the use of this data by financial institutions in the modern age, and to harness the power of data themselves in order to regulate more effectively. As well as the need for protection of sensitive personal information, this extends to strategically critical issues such as high frequency and other algorithmic trading, product pricing systems, the ability to transfer data across borders, business continuity systems and automated surveillance tools to detect misconduct. There can be no doubt that the regulation of data, and the use of data by regulators, will continue to rise in prominence in the future.

I hope that you enjoy reading these viewpoints and that they are helpful in preparing for the regulatory challenges which lie ahead.

Nathan Willmott

Head of Financial Regulation

nathan.willmott@blplaw.com

+44 (0)20 3400 4367

CONTENTS

SUPERVISION

THE SLOW BURN OF MIFID II IMPLEMENTATION - NOT OVER YET

New European rules on financial markets came into force on 3 January 2018, but full implementation is likely to take a considerable length of time. Daniel Csefalvay looks at the issues raised by MiFID II, and what firms should do to avoid unwanted attention from the regulator.

MiFID II and legal uncertainties

MiFID II introduced some of the most far-reaching and fundamental changes to the way financial markets and investment firms operate. The nature, scale and complexity of the subject-matter covered by the legislation, coupled with the overwhelming volume and complexity of the regime itself, has led to persisting legal uncertainties on certain key issues. It has also resulted in practical difficulties in implementation, particularly in the design of IT systems to handle the increased data management and new reporting obligations.

In September 2017, the FCA acknowledged these challenges and outlined an approach to the enforcement of MiFID II obligations which would be "proportionate" rather than based on strict liability. While this principle of apparent regulatory forbearance is welcome, it would be risky for firms to place undue reliance on it.

What should firms consider?

Some firms have been engaged in vast MiFID II implementation projects over several years. Others have been slower or less proactive in preparing for commencement. Accordingly, the level of compliance across the industry is varied and the FCA has acknowledged this.

In order to help mitigate the risk of FCA attention, all firms need to understand the status of their MiFID II projects, determine what gaps still exist and then undertake further implementation work to achieve full compliance. For some firms, due to their current level of compliance, this will mean continuing with full MiFID II implementation without respite until the relevant gaps have been closed.

When doing this, firms should consider the following:

→ Scoping and application issues: firms must be comfortable that all relevant provisions of MiFID II have been considered in the context of the business they undertake. Internal decisions on the application or non-application of obligations under MiFID II need to be evidenced, as does the implementation plan to give effect to those decisions.

→ Where compliance with an obligation is open to alternative interpretations – and there are many examples in MiFID II – firms should ensure they have a documented, reasonably defensible position to justify the approach they have taken to the regulator. In such cases, the FCA is less likely to take action against a firm.

→ To the extent that such matters are not appropriately documented, firms should take action without delay. The FCA has indicated on many occasions that the absence of documentation and appropriate audit trails of decision-making and subsequent implementation can lead to a presumption of non-compliance by the firm.

→ Regulatory and industry developments: the MiFID II regime will continue to evolve. The European Securities and Markets Authority (ESMA) is to publish further Level 3 guidance on a range of issues shortly. In addition, the industry's approach to costs and charges disclosure and compliance with the mandatory trading obligation for derivatives are likely to be subject to change.

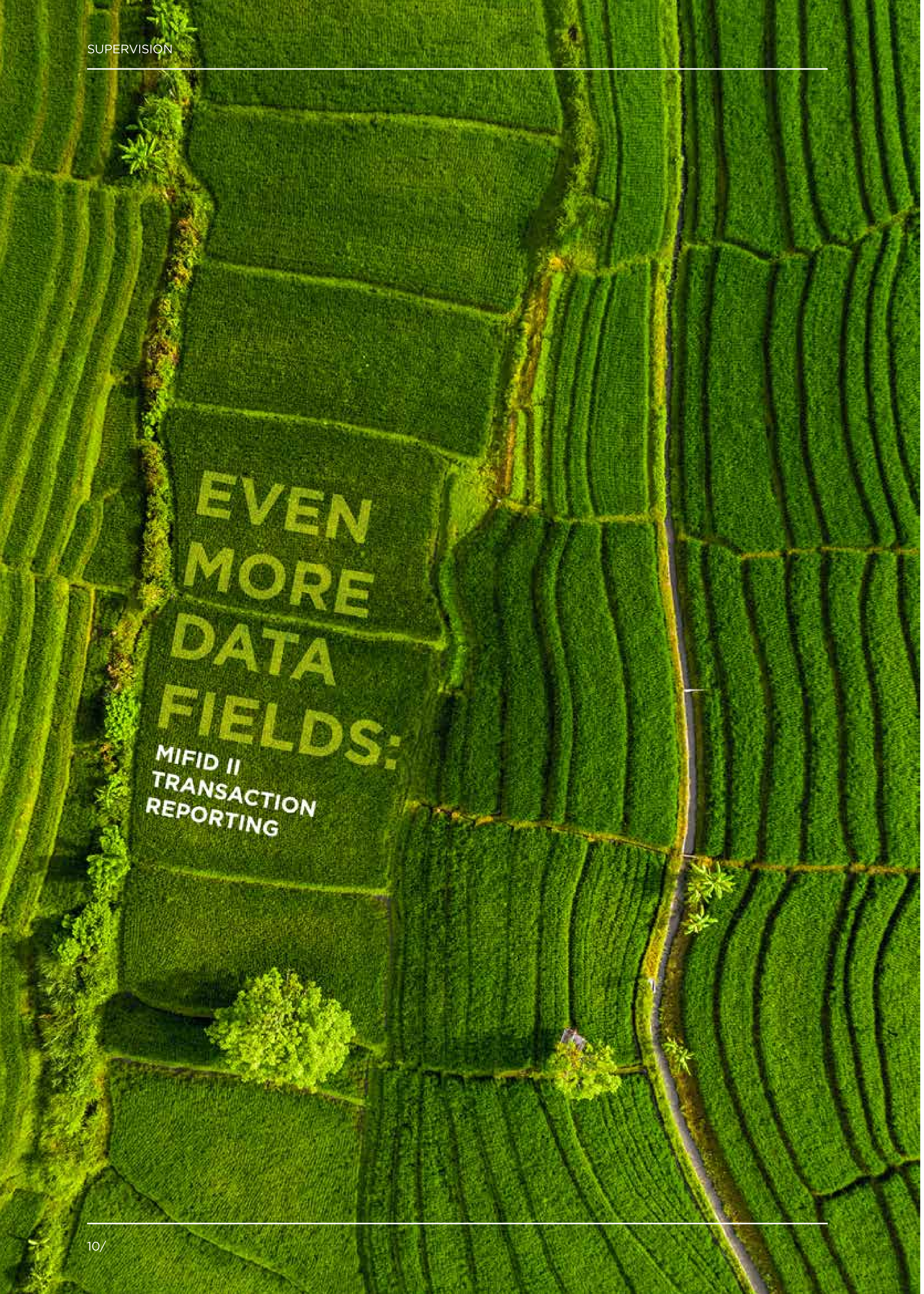
→ Firms need to ensure that their approach takes these developments into account and that, where required, appropriate changes are made to the relevant MiFID II compliance arrangements. These may include policies, procedures, IT systems and client-facing documentation. The nature of such changes could be significant, particularly where a 'correct' interpretation becomes clear, but the firm had, justifiably, taken a different stance on that particular issue.

→ Monitoring of systems and outsourcing: firms must carry out ongoing monitoring and assessment of IT systems and reporting mechanisms to ensure performance meets obligations under MiFID II. Likewise, outsourced service arrangements need to be effectively supervised by the outsourcing firm.

→ The assessment of these arrangements will be particularly important in the context of transaction reporting, transparency obligations, record-keeping and the product governance regime. The FCA has often stressed the central role that transaction reporting data plays in its fight against market abuse. It is likely that there will be less tolerance for obvious failings in this area than in some of the other aspects of MiFID II. For example, in relation to the application of the product governance rules to vanilla private side capital raisings, technical differences in approach may not necessarily undermine the regulatory objectives of the regime in such a clear way.

MiFID II has already imposed an immense burden on the financial services industry. Nevertheless, firms will need to continue to devote significant resource to implementation and to consult external advisors in order to avoid regulatory scrutiny and, in a worst case scenario, potential enforcement action.

Daniel Csefalvay
Partner, Financial Regulation



EVEN MORE DATA FIELDS: MIFID II TRANSACTION REPORTING

As the dust settles on MiFID II implementation, Anthony Williams looks at the impact of the new transaction reporting regime. The previous rules were not easy to follow, with many firms incurring fines for transaction reporting breaches. The new system will be even more challenging. What is changing, and why?

Time is officially up on the race to put the 1.5 million paragraphs of MiFID II into practical effect. Now that the 3 January deadline has passed, late-finishers may take some comfort from the FCA's signals that it will not immediately pursue enforcement action against non-compliant firms, as long as they have made a real effort to implement the requirements.

One area that has caused a monumental headache for Compliance, IT and Operations teams across the financial services sector is the revised transaction reporting regime. The new requirements ratchet up the complexity from the previous set of rules. There is more to report on more transactions in more instruments by more firms and the number of reportable data fields has leapt from 23 to 65. Among other things, the new reports must identify the individual and/or computer algorithm responsible for each investment decision and the execution of the transaction.

An implementation headache

For firms that trade many types of instruments across multiple front, middle and back office systems, the implementation process has been painful. In many cases, a complete overhaul has been necessary.

It is not as if firms found compliance with the previous regime easy. The FCA imposed fines totalling over £33m for transaction reporting breaches under MiFID I. Common failings included reporting incorrect trade times, identifying the wrong counterparties, mixing up buy/sell indicators, and using incorrect instrument identification codes. Given the extended data requirements, accurate reporting under the new rules will be even more of a challenge. Robust quality assurance and reconciliation controls are a must.

£33m fines imposed by the FCA for transaction reporting breaches under MiFID I

£50m spent by the FCA on a new transaction-monitoring system to process data gathered under MiFID II

Tackling market abuse is a priority

While firms will have their hands full complying with the new regime, the FCA is hoping to put the data it receives to good use. The FCA has spent almost £50m developing a new transaction-monitoring system capable of processing the extra information. As a result, it will have a better view of the market than ever before.

All this work has been directed at one main goal: the prevention and detection of market abuse. The FCA repeatedly emphasised last year that market abuse is now a priority for its Enforcement Division, and there was a large uptick in the number of related investigations. We can expect this trend to continue in 2018, as the enhanced MiFID II transaction reporting data will enable the FCA to subject trading activity to even greater scrutiny.

“Given the extended data requirements, accurate reporting under the new rules will be even more of a challenge. Robust quality assurance and reconciliation controls are a must”

Anthony Williams
Associate,
Financial Regulation

WILL THE IDD STOP GOLD PLATING INSURANCE DIRECTIVES?

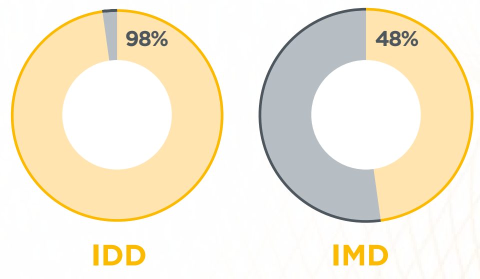
Next year sees the repeal and replacement of the EU's IMD in an attempt to create a more consistent environment across EU Member States. The Member States have until 23 February 2018 to transpose IDD into national law, though latest developments mean firms may not need to apply it until 1 October 2018. In the UK, the process is well underway. Martin Griffiths asks, will this change the insurance market and will gold plating be a thing of the past?

What is the IDD?
Following a review of the operation of the Insurance Mediation Directive (IMD), the European Commission concluded that it had been inconsistently applied across Member States, with some States gold plating measures and others implementing the bare minimum.

The Insurance Distribution Directive (IDD) is an attempt to solve these issues and create a level playing field for all entities selling insurance and improving regulation in the retail insurance market. Despite inconsistent application being the main reason for revising the IMD, the IDD is still (strangely) a minimum harmonisation directive, so Member States are free to implement more stringent requirements.

What is going to change?
The IMD covers insurance intermediaries only. In contrast, the IDD also applies to the direct sales forces of insurers. With its usual passion for gold plating, when the UK implemented the IMD it chose to bring insurers and reinsurers as well as insurance intermediaries within scope, so this extension is not a significant one in a UK context.

> At a pan-EU level the change is significant, as the IDD covers approximately 98% of the market, compared to the approximately 48% covered by the IMD



Unlike the IMD, the IDD also expressly applies to aggregator/price comparison websites. Firms running such websites will need to be registered with the competent authority in their home Member State. Again, this is not a significant change for the UK, which already requires these firms to be authorised.

The IDD retains (with a few small changes) the connected contracts exemption contained in IMD, that applies to certain add-on products sold as a package by a firm whose principal business is not the distribution of insurance products. These firms will be outside the scope of the IDD.

The current UK connected contracts exemption is not as broad as the one contained in IMD, in that it does not extend to travel insurance sold as a part of a package alongside a package holiday or to motor vehicle warranties. HM Treasury has concluded that it is minded to continue this gold plating approach with the IDD exemption. The IDD imposes an obligation on insurers selling through exempt intermediaries to ensure that those intermediaries comply with certain conduct rules.

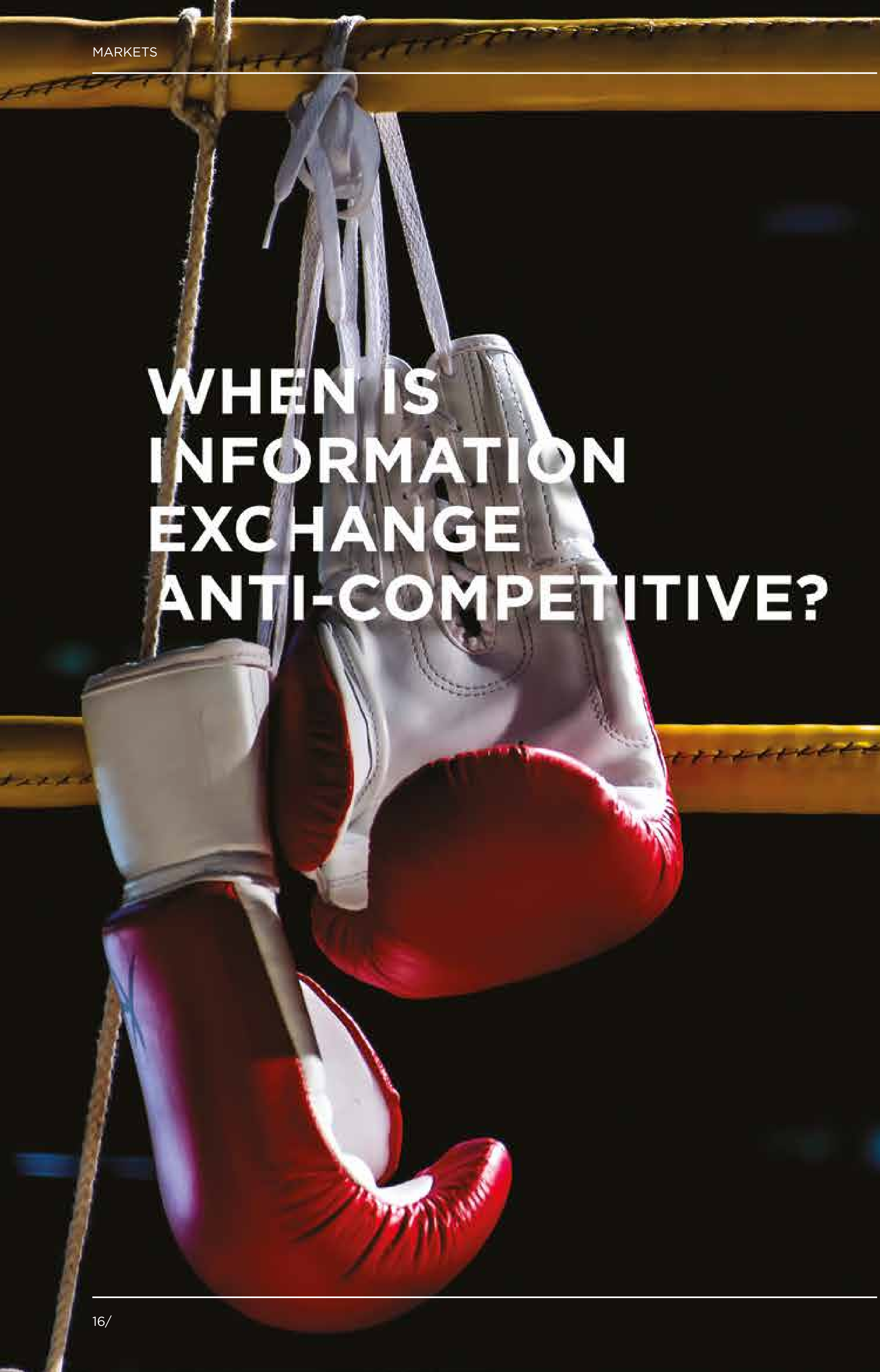
The IDD includes requirements that were not in IMD in relation to: professional training for insurance distributors and their employees; the conduct of business by insurance distributors; the management of conflicts; cross-selling; and the distribution of insurance based investment products (such as unit-linked policies, with-profits policies and investment-linked income annuities). However, it is clear from the FCA consultation papers that the UK requirements are unlikely to change drastically because the FCA Handbook already covers, to greater or lesser extents, many of these requirements. Indeed, some of the changes the FCA propose to make amount to not much more than a change in layout of the Handbook, so thatrelated distribution rules can be found in one place.

Will Brexit change anything?
The HM Treasury consultation paper acknowledges that the outcome of the Brexit negotiations will determine what arrangements will apply in relation to EU legislation (such as the IDD) once the United Kingdom has left the EU. However, given many of the requirements of the IDD are already part of UK law or regulation (and in some instances gold plated), it seems unlikely that Brexit will mean a material divergence from the requirements of the IDD, at least in the short to mid-term.

Martin Griffiths
Senior Associate, Corporate Insurance

MARKETS


LEGAL AI
INITIAL COIN OFFERINGS
DIFC
SMCR
LEGAL AI
FORENSIC TECHNOLOGY
IDD
MIFID II
DPR
MIFID II
FINANCIAL CRIME
BREXIT



WHEN IS INFORMATION EXCHANGE ANTI-COMPETITIVE?

As the FCA takes forward its first Competition Act case since being granted concurrent competition powers in 2015, information exchange has emerged as a key area of focus for the regulator. Sarah Ward and Victoria Newbold consider when information exchange among competitors can give rise to a competition law risk, and what firms can do to avoid breaching the rules.

A complex area of law

It is a common misconception that competition law infringements are limited to hardcore cartel behaviour. Many do not realise that the competition law rules also prohibit the exchange of commercially sensitive information between competitors, except to the extent strictly necessary to implement a legitimate commercial arrangement. This area of law, and the line between appropriate and inappropriate behaviour, is significantly more complex and difficult to navigate.

Information exchange also poses a particular risk for regulated firms, who may frequently be involved in arrangements such as joint financing, co-insurance or loan syndication which require competitors to work together and share information. Other established practices that can help financial markets to operate more effectively, such as the sharing of market colour or benchmarking, can easily cross the line into inappropriate conduct.

The FCA has already started looking into such practices. In 2016, it sent "on notice" warning letters to a number of competing syndicated lenders it suspected of having exchanged information on the terms and conditions of their loans. Most recently, in April 2017, it carried out dawn raids on insurance brokers active in the aviation sector, apparently as a result of the brokers' exchanges of commercially sensitive information, an investigation which has since transferred to the European Commission. In late November 2017, the FCA announced its first ever competition law enforcement case, issuing provisional findings in the form of a "statement of objections" against four London-based asset management firms for allegedly exchanging pricing information in connection with two IPOs and a placing in 2014 and 2015.

> Between 2013 and 2016, the European Commission imposed fines of over €2bn on banks for participating in the Swiss Franc Libor, bid-ask spread, EIRD and YIRD cartels

What are the rules?

Firms are prohibited from disclosing or exchanging commercially sensitive information with competitors, except to the extent necessary to achieve relevant benefits for a client. Such benefits may include obtaining finance or insurance, which they would not otherwise obtain because, for example, the product can only be provided jointly by a number of banks or insurers who need to exchange certain information in order to provide it.

What amounts to commercially sensitive information will differ from case to case, but typically includes any information which could reduce strategic uncertainty between competitors, such as current or future prices, quotes, margins, revenues and commercial strategies.

Where firms receive commercially sensitive information from competitors and remain active in the market thereafter, they are presumed to take account of that information in determining their future conduct in the market. This can amount to an anti-competitive agreement or concerted practice in breach of the competition law rules.

In recent years, firms have faced significant penalties for engaging in information exchange that has supported price fixing and market manipulation. For example between 2013 and 2016, the European Commission imposed fines totalling over €2bn on banks for participating in the Swiss Franc Libor, bid-ask spread, EIRD and YIRD cartels. In 2014 and 2015, six banks were fined over $5.5bn by global regulators, including the FCA, for the manipulation of foreign exchange benchmarks. Even in the absence of actual agreement, competition authorities are not afraid to impose large fines on firms engaging in inappropriate information exchange. For example, the Office of Fair Trading imposed a fine of £28m on RBS in 2011 for the unilateral disclosure of confidential and commercially sensitive future pricing information to Barclays with the aim of coordinating the price of loans supplied to large professional services firms.

Information exchange need not be direct

It is also possible for competitors to breach the rules by sharing information via an intermediary, such as a broker, a trading platform, the operator of a shared database, or a client. In 2015, the European Commission fined UK-based broker dealer ICAP €14.9m for participating in cartels in the Yen interest rate derivatives sector as a 'cartel facilitator', in part because it served as a communications channel for Citigroup and RBS traders to share information relating to trading positions and future LIBOR submissions.

How can firms protect themselves?

It is important to consider whether existing training and guidance for staff is sufficient to manage the risks associated with information exchange, and what procedures may be appropriate to minimise the risks associated with legitimate commercial practices which involve contact with competitors.

General good practice will help to avoid some of the most obvious mistakes in this area. Consider whether your client would agree to you sharing the information, and whether it is being shared for a legitimate purpose. Be cautious with your choice of words to avoid the possibility that you could be accused of impropriety. If you receive information which you consider to be inappropriate, be sure to distance yourself from the disclosure. Finally, creative use of internal information flows and ring-fencing can help prevent inappropriate information disclosure in the first place.

> In 2014 and 2015, six banks were fined over $5.5bn by global regulators, including the FCA, for the manipulation of foreign exchange benchmarks.

KEY DOS AND DON'TS:

- Consider creative solutions to manage internal information flows, such as ring-fencing, and/or the use of NDAs
- If you receive information which you consider may be inappropriate, or are present when such information is disclosed, distance yourself from the disclosure
- Ensure that all contacts with competitors are for a legitimate purpose

- Don't be flippant with your language – careless words can create the appearance of impropriety and can be difficult and costly to explain or defend
- Don't exchange commercially sensitive information with competitors over that which makes it necessary for a legitimate commercial arrangement
- Don't forget to put yourself in the client's shoes – consider how they would feel if they knew that the information in question had been shared

Sarah Ward
Senior Associate,
Antitrust &
Competition

Victoria Newbold
Associate,
Antitrust &
Competition

HURRY UP OR WAIT?

Months after firing the starting pistol on Brexit negotiations, we are no further forward in understanding the practical impact for the UK financial services industry. The PRA has not revealed much about its plans, although it expects firms with cross-border EU activities to have contingency plans. Geraldine Quirk and Adam Bogdanor look at the range of possible outcomes that firms need to consider.

UK insurers – to relocate or not?

For UK insurers with live underwriting operations covering EU risks, the only way to guarantee continuation of that business post-Brexit is to set up a vehicle in the EU. A number of large insurance groups have taken this approach. There is no clear front-runner in terms of favoured jurisdictions, with Luxembourg, Belgium, and Ireland all being chosen.

The costs of setting up in another EU state are likely to be significant. For those hoping to have a lean operation with significant outsourcing back to the UK, the European Insurance and Occupational Pensions Authority (EIOPA) fired a warning shot in its guidance to EU supervisors. EIOPA wants to ensure convergence in approach, to avoid UK insurers being incentivised to favour one state over another when deciding where to set up. It expects supervisors to require an appropriate level of local corporate substance for new insurers, and a level of local staff proportionate to the insurer's business. This hardening attitude to supervisory convergence seems to be a theme, making it increasingly difficult for supervisors to exercise discretion in the interpretation of EU rules.

A fronting arrangement may be an option, although EIOPA wants supervisors to require a minimum retention in the fronting entity of 10% of the business written. Unless the EU grants the UK equivalence for reinsurance, the EU fronter may not be able to take full credit for the reinsurance in calculating their SCR, unless collateral is provided, which may make these arrangements unattractive. Collateral would be essential in any case to reduce counterparty default risk.

For existing business, the hope is that insurers will be able to continue to administer claims under existing policies covering EU risks from the UK. Anything else would be contrary to policyholder interests. As with so much on Brexit, there is no formal position on this. While insurers could choose to transfer EU risks to an EU insurer, this can take 18 months and there is no guarantee that it would be complete before March 2019. For some, a solution may be to convert to a SE by setting up and merging with a shell EU company, migrating the SE to an EU state and administering any UK risks from outside the UK. Depending on the nature of the business and the approach of the regulator in the target jurisdiction, this could take less time than a Part VII transfer.

Adam Bogdanor
Partner, Corporate Insurance

Geraldine Quirk
Partner, Corporate Insurance

Incoming insurers

The Bank of England expects to make an announcement by the end of 2017 (not yet published at the time of going to press) on whether UK branches of EEA firms will be allowed to become third country branches, or whether a subsidiary will be required. We are expecting that firms with UK operations below a certain size will be able to operate through a branch, with larger operations being required to subsidiarise. Pre-Brexit, there is no mechanism for an EU insurer to apply for branch authorisation. We expect that provision will be made for a pre-application process so that firms can begin to prepare, and the regulators can consider applications in advance of March 2019.

Incoming EU insurers may question whether the additional regulation and capital requirements in keeping separate UK and EEA businesses are worthwhile if their UK business is small or non-core and, if not, they will likely dispose of their UK business.

Whatever contingency plans firms decide to adopt, there is a justifiable concern that the UK regulators will struggle to deal with the inevitable flood of applications in time (whether for authorisation, approval of change of control or a transfer). Restructuring EU business following Brexit is likely to become more complex. Mutual recognition of transfers will cease and mechanisms such as cross-border mergers and the formation and migration of a European company will no longer be available, in the absence of an agreement to the contrary.

So while firms may feel that the best strategy is to wait and see, there is a risk that by the time the future rules for cross-border operations are clearer, restructuring options may be far more limited.

> “For existing business, the hope is that insurers will be able to continue to administer claims under existing policies covering EU risks from the UK. Anything else would be contrary to policyholder interests”

INSURANCE BROKERS UNDER THE MICROSOPE

On 8 November, the FCA published details of a market study into the wholesale insurance market. Using its wide-ranging powers under the FSMA, the FCA is seeking to identify any structural competition, consumer or market integrity issues in this market. Andy Hockley and Julia Joseph explore what the FCA is really interested in, and what this might mean for the industry.

> If the market study reveals regulatory breaches or other improper conduct by specific firms or individuals, it could lead to formal investigations under the FSMA

The UK's wholesale insurance market commands significant revenues, both for insurers/reinsurers and for brokers. With more than $91bn in gross written premium in 2015, the London market is one of the biggest global centres for placing and underwriting large-scale, complex, commercial and specialty risks.

The FCA notes the crucial role that brokers play in this market to ensure their clients get the coverage they need at a competitive price.

The wholesale insurance market was last reviewed in any detail in 2007 by the FCA's predecessor, the Financial Services Authority. Since this time, the sector has undergone some radical changes, prompted in part by a prolonged "soft market" in which premiums have continued to decline. The FCA is concerned that these market conditions may have resulted in some broker behaviours (such as increased use of facilities and the provision of additional broker services) that may be restricting competition and preventing the market from operating as well as it could in the interests of clients.

The launch of this market study follows soon after it was announced that the European Commission had seized jurisdiction over the FCA's high-profile competition investigation into aviation aerospace insurance and reinsurance broking, which hit the news following dawn raids in April 2017. Having lost its ability to scrutinise specific allegations of competition law infringements in the aviation insurance broking sector, the FCA is now using its Financial Services and Markets Act 2000 (FSMA) powers to carry out a far-reaching study of the entire wholesale sector.

> The London market is one of the biggest global centres for placing and underwriting large-scale, complex, commercial and specialty risks

What's in focus?

The FCA has cast its net widely to cover wholesale insurance and reinsurance for large, complex or specialist risks placed by brokers in the London insurance market, with a focus on large corporate clients based both in the UK and overseas.

1. **Market power** – the FCA is considering whether individual broker firms possess market power and, if so, whether this is harming competition (for example, because brokers are using this market power to seek enhanced commission or to get underwriters to take up additional products and services).

2. **Conflicts of interest** – there is concern that a lack of transparency and the asymmetry of information between clients and brokers is resulting in conflicts where the client may lose out to the interest of the broker. In particular, the FCA is considering the following questions:

   - Do brokers place business within facilities that may yield greater remuneration to the broker, even if this is not in the best interests of their clients?
   - Are brokers more likely to place underwriting business with insurers that purchase data and other advisory services from them? Do they insist on any reinsurance from an insurer being placed with the same broker even if this is not in the best interests of their clients?
   - Are brokers channelling business to their in-house Managing General Agents to retain a greater share of the premium revenue on risks they place?

3. **Broker conduct** – finally, the FCA will examine certain broker practices that may have an impact on competition. In particular, the FCA will be looking at:

   - Whether brokers are excluding some insurers by placing risks through facilities, rather than on the open market.
   - Whether there has been a dampening of competition between brokers through "tacit" coordination. Specifically, the FCA is looking at whether the sharing of pricing data and other client information via third party intermediaries makes it easier for brokers to coordinate their behaviour. In this regard, the FCA may be influenced by knowledge and experience already gained in its competition investigation in the aviation insurance broking sector.

The FCA expects to publish interim conclusions in autumn 2018, with a final report due in late 2019. If the FCA concludes that competition is not working well, it has wide-reaching powers to intervene, for example, by imposing market or firm-specific remedies.

Remedies imposed by the FCA can extend beyond the scope of the initial market study. The FCA's general insurance add-ons market study, for example, led the FCA to introduce rules to ban "opt-out selling" across all financial services sectors, not just those covered by the market study, from 1 April 2016.

Should the FCA identify potential infringements of other laws, such as competition law, it may open an investigation or refer the matter to other enforcement agencies. Similarly, if the market study reveals regulatory breaches or other improper conduct by specific firms or individuals, it could lead to formal investigations under the FSMA.

If the FCA concludes that a more detailed study is warranted, it may also refer the sector for a more detailed "market investigation" by the Competition and Markets Authority (CMA). The FCA is not afraid of taking this step, having done so in September 2017 when it made a market investigation reference for investment consultancy services following its asset management market study. The CMA has a wide range of remedies it may use to address any adverse effects on competition that it identifies during a subsequent investigation, including requiring divestment of a business or assets.

An opportunity to engage

The FCA consulted on the scope of its review during December and January. The FCA has sent detailed requests for information to brokers and insurers for response in Q1 2018.

It is intending to publish its provisional findings in autumn 2018, and would welcome engagement before that date. This is a valuable opportunity to table concerns with a view to them being addressed in a non-firm specific context.

Julia Joseph
Senior Associate, Antitrust & Competition

Andy Hockley
Partner, Head of Antitrust & Competition

FCA COMPETITION ENFORCEMENT – THREE PREDICTIONS FOR 2018

The FCA has shifted its focus from market studies to tougher enforcement methods, including antitrust 'dawn raids' and on-site inspections. How will enforcement strategy change during 2018? James Marshall and Marieke Datema have three insightful predictions.

A uniquely powerful regulator

The FCA became a concurrent competition regulator in April 2015. This means the FCA can conduct competition -oriented market studies under both competition and financial services legislation, as well as investigate and enforce suspected breaches of competition law under the relevant competition statutes.

The FCA continues to carry out market studies, but has now shifted its focus to individual enforcement cases, including conducting its first antitrust 'dawn raids' during 2017. The FCA has demonstrated that it is willing to use its Competition Act 1998 investigation powers and has also been clever in its use of 'soft enforcement' tools. We expect this trend to continue.

The increased use of individual enforcement tools also highlights the importance of notification obligations under the FCA Handbook. We expect the mode and procedure for notification of potential competition law issues to become an increasingly sensitive issue in 2018.

THREE PREDICTIONS FOR 2018

1. More moderate use of market studies as the FCA prioritises investigations and enforcement activity.
2. More individual firm enforcement using both hard and soft enforcement powers.
3. Increased focus on strategies for FCA notification and wider competition risk assessments.

THE TRENDS WE PREDICT FOR 2018

More moderate use of market studies
FCA market studies serve two purposes in particular:

1. To identify structural competition, consumer or market integrity concerns. Where necessary, the FCA may seek regulatory changes or structural reforms to address its concerns.
2. To identify behaviours and practices by individual firms that it may wish to investigate using its hard or soft enforcement powers.

FCA market studies have been the most visible aspect of the FCA's competition agenda. FCA studies have covered areas including wholesale banking, retirement outcomes, credit cards and asset management. Ongoing FCA market studies include residential mortgages and investment platforms. In November 2017, the FCA launched a market study in the wholesale insurance subsector.

The FCA's wholesale insurance broker study is far-reaching (covering wholesale insurance and reinsurance for large, complex or specialist risks placed by brokers in the London insurance market), and has the potential to have a significant impact on the regulation of the sector going forward. Although the FCA had indicated in April 2017 its intention to review the wholesale insurance sector, the timing of the market study is notable as it took place soon after it was announced that the European Commission had seized jurisdiction over the FCA's competition investigation into aviation and aerospace insurance and reinsurance broking. This market study may be a way for the FCA to ensure it retains a role in scrutinising potentially anti-competitive behaviours in the wider wholesale insurance sector.

The FCA has also made its first market investigation reference to the Competition and Markets Authority (CMA), relating to investment consultancy and fiduciary management services. The CMA has extensive powers in a market investigation context, and potential outcomes of the CMA's detailed 18-month review could include forced divestitures or other major interventions.

The FCA will continue to use market studies as an important tool. However, we expect to see lower rates of market studies in the year ahead, with the FCA prioritising investigation and enforcement activity instead.

More individual firm enforcement – information exchange in focus
The FCA has been an active competition enforcer since launching its first Competition Act 1998 investigation in early 2016. This investigation is ongoing, and details remain confidential.

As mentioned on page 17, in April 2017 the FCA commenced its second Competition Act 1998 investigation when it conducted dawn raids at the offices of five major aviation insurance brokers. Although the European Commission has now seized jurisdiction over this investigation, carrying out on-site inspections sends a strong signal that the FCA is prepared to use intrusive investigation tools, as well as its full range of general competition enforcement powers. We anticipate that the FCA will continue its proactive competition enforcement activities in the coming year.

We also expect the FCA to build on its use of soft enforcement methods. In 2016/17, the FCA issued 23 'on notice' letters and six advisory letters. These letters identify potential competition issues, and can transfer some of the burden of investigating and remedying competition problems from the FCA to individual firms. These tools are an effective means of freeing up scarce FCA resources to focus on priority areas, and we expect their use to grow.

In terms of substantive areas of focus, illegal information exchange will continue to be a priority area for the FCA in 2018, as explored further in our article 'When is Information Exchange Anti-competitive?' (page 16).

23 'ON NOTICE' LETTERS AND 6 ADVISORY LETTERS ISSUED BY THE FCA IN 2016 – 2017

Procedure for, and mode of, notification to the FCA will be key
The FCA Handbook (SUP 15.3.32R(1)) requires firms to notify the FCA of any significant infringement (or potential infringement) of any applicable competition law – including infringements of competition law outside the UK. Regulated firms also have wide-ranging self-reporting obligations under conduct regulations, including the broad Principle 11 duty.

If the relevant conduct is sufficiently serious, the FCA's mandatory self-reporting obligation may, in effect, also force a firm to seek antitrust leniency.

In the year ahead, we expect the FCA to require firms to affirm the rule(s) under which a notification is made. If firms have to self-report potential competition issues expressly or exclusively under SUP 15.3.32R(1), this may affect their strategies for notification and wider competition risk assessments of the relevant conduct. In turn, this could make FCA regulated firms more vulnerable to competition sanctions and possible damages actions than non-FCA regulated peers would be in a similar situation.

Continue to expect focused enforcement
We expect the FCA to continue to use its full range of competition powers in 2018. Our experience suggests that, as well as domestic enforcement, the FCA will continue to work closely with overseas peer regulators in cross-border investigations, demanding coordinated case management for firms under investigation.

> "The FCA has now shifted its focus to individual enforcement cases – including conducting its first antitrust 'dawn raids' during 2017"

Marieke Datema
Senior Lawyer Consultant, Antitrust & Competition

James Marshall
Partner, Antitrust & Competition

DIGITAL

TO DELETE OR NOT TO DELETE?

THE CONFLICTING PRESSURES OF DATA RETENTION

Companies are being pulled in different directions over data. On the one hand, the more data you hold, the greater the risk of a damaging information leak; on the other, data is valuable and can help support your case if accused of wrongdoing. Regulation in this area is also about to become more complex with the introduction of the GDPR. Oran Gelb and Joseph Ninan look at why you might keep or delete data, and how to reduce your risk.

> "The fact of conflicting interests in keeping data or weeding it out is not a new issue. However, the conflict is becoming increasingly acute and burdensome for firms to manage"

For many years, financial institutions have been compulsive data hoarders. There are at least three reasons for this:

1. **Regulatory obligations** – there are many regulatory rules which impliedly or expressly require firms to retain data, e.g. SYSC provisions on record-keeping, obligations to provide regulatory references, AML requirements, surveillance and reporting obligations under MAR, etc.
2. **Investigations** – we are now in an enforcement climate where past conduct is frequently scrutinised and investigated. Firms and individuals need data to investigate issues, respond to regulators and/or defend themselves.
3. **Practicality** – the sheer volume of data that is now generated by financial institutions and embedded within their complex – often legacy – systems makes it difficult to destroy.

On the other hand, we are now experiencing unprecedented numbers of data breaches. There is some logic to the simple notion that the more data a firm holds, the more exposed it is to such breaches.

In addition, the General Data Protection Regulation (GDPR) comes into force on 25 May 2018. Although many of the substantive rules are similar to those under the current Data Protection Act, there is an even greater emphasis on data minimisation, i.e. only retaining personal data for as long as is necessary. The GDPR will also provide the Information Commissioner's Office with effective teeth to enforce data protection, with mandatory breach reporting and much-publicised fines of up to €20m, or 4% of turnover.

The fact of conflicting interests in keeping data and weeding it out is not a new issue. However, the conflicts are becoming increasingly acute and burdensome for firms to manage.

HOW TO REDUCE YOUR DATA RISK

- Review policies which require blanket retention of data for longer than legally required
- Switch to systems that delete data completely rather than archiving it
- Enforce rules on communication channels, such as email and chat being for business only
- Set dates for deletion of sensitive personal data from sources, such as HR records

Data minimisation

Under the GDPR, firms will need to identify a route that allows them to process personal data. They have always had to do this under the Data Protection Act, but the choices have now narrowed. In particular, more stringent requirements attached to "consent" mean that firms will be less inclined – and able – to rely on the consent of the data subject. The GDPR clarifies that pre-ticked opt-in boxes are not active indications of valid consent, nor are terms and conditions in an employment contract.

Firms also need to make it as easy for consent to be withdrawn as it was to provide it in the first place. In short, firms will need to rely on another rationale to process personal data. It is likely that the processing is necessary for compliance with the data controller's legal obligations (Article 6(1)(c)) or necessary for the purposes of legitimate interests pursued by the controller balanced against those of the individuals concerned (Article 6(1)(f)).

The GDPR also introduces the concept of the 'right to be forgotten' and 'privacy by default'. Both of these concepts will require companies to take measures to ensure they do not continue to retain personal data after it ceases to be required.

Data retention

Conversely, there are an increasing number of regulations that are pulling firms in the opposite direction of data retention. Take the example of regulatory references under the SMCR. Firms are now required to provide a reference for ex-employees for anything that occurred within six years of a reference request. Firms will also have to disclose serious misconduct, no matter when it occurred.

These obligations mean that firms must have in place policies and procedures that ensure the relevant records are kept for at least six years and, in the case of serious misconduct, indefinitely. After these time periods are up, firms must also have policies and procedures for removing or redacting any personal data.

The Money Laundering Regulations also impose data retention requirements on firms: Article 40 of the new 2017 regulations requires firms to retain all customer due diligence and transaction records for a period of five years from the date the business relationship terminates or, in respect of occasional transactions, from the date the transaction is complete. Once again, the onus is on the firm to monitor this time period and take appropriate steps to remove personal data at the end of it (Article 40(5)). Similarly, there is also a five-year period for record-keeping under MAR.

These are just a few of the many examples of data retention obligations embedded into regulatory requirements.

Data for the defence

It can also be in a firm's interests – and those of its senior management – to retain records in today's enforcement and litigation climate. It is an age-old debate amongst defence lawyers as to whether a client is better off having documents or not when faced with claims and investigations. Clearly, the circumstances will differ and some documentation may be harmful rather than exculpatory. Greater volumes of data can also be expensive to store and (if required) disclose in a dispute or regulatory process.

However, in our experience it is often helpful to be armed with relevant information and documents, particularly when dealing with regulatory scrutiny. The FCA is not easily persuaded that the correct approach was taken where there is no documentary evidence to support it.

The new approach to enforcement under Mark Steward means the threat of an investigation is now greater than ever. There is also now a longer limitation period of six years (from the date the FCA identified the breach) for the FCA to bring an enforcement action against an individual. No limitation period applies to prohibitions against individuals, and the current focus on individual accountability may see that power being invoked more readily. This is seen in the ongoing investigations into the former senior managers of HBOS despite the six-year time limit elapsing.

> "It is an age-old debate amongst defence lawyers as to whether a client is better off having documents or not when faced with claims and investigations"

Practical implications

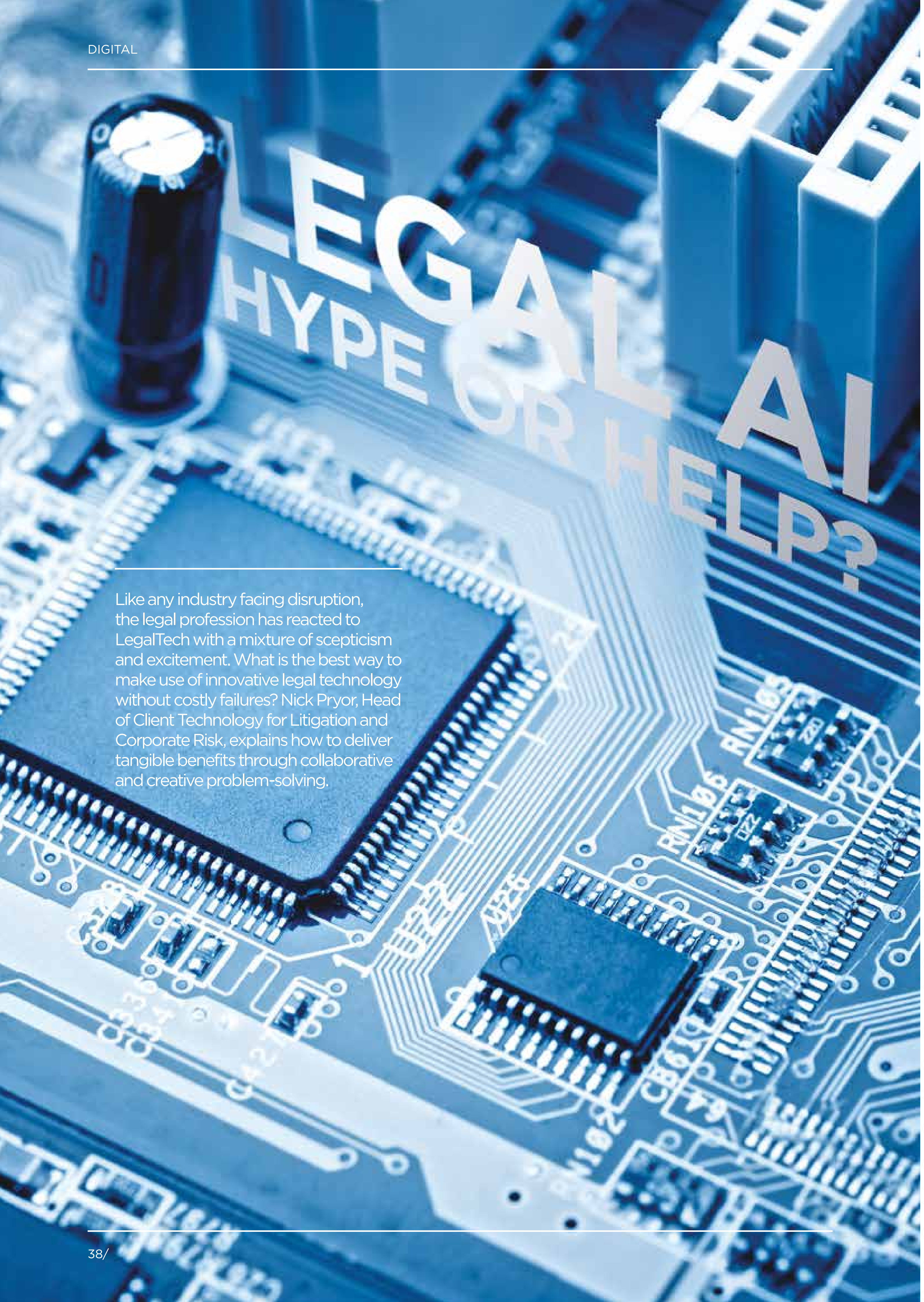
We think firms and senior management will continue to hang on to data for periods beyond their strict legal obligations. This will stretch the outer bounds of the 'legitimate interests' exception for processing personal data, and we can see the prospect of a case in the post-GDPR world that will challenge these practices.

For now, firms may want to revisit policies and processes in order to see whether there is anything they can do to mitigate their risk without unduly prejudicing their interests.

1. Reconsider blanket retention policies for periods significantly in excess of legal requirements. Where issues arise, firms can then suspend document destruction policies.
2. Introduce systems which remove electronic data completely, rather than archiving it. We are aware that firms have adopted this approach for voice recordings, but they are less common for written electronic communications.
3. Enforce strict policies on staff using business communication methods (e.g. emails, Bloomberg chat, etc) for business purposes only, thereby reducing the risk of storing irrelevant private and possibly sensitive personal data.
4. Exercise particular vigilance to remove sensitive personal data after limited periods of time (e.g. HR records on staff health issues).

Oran Gelb
Partner,
Commercial
Dispute Resolution

Joseph Ninan
Associate,
Financial Services
Investigations



LEGAL AI

HYPE OR HELP?

Like any industry facing disruption, the legal profession has reacted to LegalTech with a mixture of scepticism and excitement. What is the best way to make use of innovative legal technology without costly failures? Nick Pryor, Head of Client Technology for Litigation and Corporate Risk, explains how to deliver tangible benefits through collaborative and creative problem-solving.

LegalTech goes mainstream

LegalTech, and its fellow disruptors FinTech, RegTech and InsurTech, have gone from niche sidelines to major headlines in very short order. Every financial institution and professional services firm is alive to the new opportunities opened up by tech startups and enterprise players alike.

The level of hype around applied technologies, and legal AI in particular, provokes strong reactions – from exhilaration, to scepticism or even fear. The healthiest response is probably a combination of all three. Some of the hype is overblown, with apocalyptic mainstream press articles heralding the advent of "Robot Lawyers". This reductive and unhelpful narrative risks undermining the genuine and immediate benefits and opportunities of the true state-of-the-art technology.

Riding out the hype cycle

IT firm Gartner illustrated the maturation of new industry technologies in terms of a Hype Cycle moving through five phases:

- **Phase One:** a "technological trigger". In the LegalTech space, this was the development of new machine learning techniques applicable to legal business requirements. This gives rise to some early partnerships, and well-publicised success stories. Our development of "LONald", in partnership with RAVN, is a well-documented case study in this regard.
- **Phase Two:** a "peak of inflated expectations". Early successes precipitate a giddy overreaction within the industry. There is a tendency to oversimplify the technology, and extrapolate out to imagine impossible returns.
- **Phase Three:** the "trough of disillusionment". Misconceived applications of the technology and some costly failures cause interest to wane, and for some businesses to dismissively de-prioritise their commitment.
- **Phase Four:** the "slope of enlightenment". Those who persevere and deploy the technology appropriately start to thrive. This is compounded as the underlying technologies mature, and deliver more dramatic returns. Arguably, predictive coding in e-discovery has reached this phase of deployment.
- **Phase Five:** the "plateau of productivity". This is the end state phase, where the technologies have truly matured and become mainstream, with well-understood application and returns.

How to harness the potential of LegalTech

What is the best way to navigate this hype cycle without overestimating or underestimating the transformative potential of LegalTech? The trick is to recognise that the technology is never anything more than an implementation detail, it is a means to an end, and not an end in its own right. Never start by questioning how to leverage an intriguing new technology, the starting position should always be examining how a particular problem can be solved more creatively, and then evaluating how technology might feed into that solution.

Taking a disciplined, results-oriented approach to legal AI requires three things:

1. **A deep understanding of the LegalTech market,** and strong relationships with all the significant service providers. The market is moving quickly, and it is our responsibility to understand which technologies provide genuinely compelling practical solutions, and which ones will fail to deliver.
2. **A strong appreciation for what each platform can – and more importantly cannot – do.** AI can be very powerful, but it is never a "silver bullet" solution. Every technology has different challenges and limitations, and all of them require a significant investment of data, training, and legal expertise in order to deliver meaningful results.
3. **Close cooperation between lawyer and client.** Every successful application of legal AI results from a smart marriage between the right technologies and the right kinds of problems; making that match requires a diversity of perspectives, and a collaborative spirit. AI tools sometimes work in counterintuitive ways, and often the problems that feel hardest to solve are actually the easiest, and vice versa.

We are passionate about the capacity for AI to deliver excellent, innovative solutions to complex legal problems. In the software industry, technical solutions are usually born out of "ideation" sessions. In more traditional industries, this would be simply known as "brainstorming". Whatever you choose to call it, our team is always willing to work with you to understand the challenges you face, and highlight how our range of applied AI tools and legal expertise can help you solve problems in new and better ways.

Nick Pryor
Head of Client Technology for Litigation and Corporate Risk

CAN WE LEARN TO LOVE THE GDPR?

> Companies with access to a customer's account and transaction data as well as a credit score can provide tailored offers that more accurately reflect their individual circumstances

Will the GDPR help to fuel innovation in the consumer financial services market, or stifle it? As new consumer data laws come into force in 2018, Kate Brimsted and Tom Evans look at what the changes mean for personalised consumer offers, marketing and risk management.

What is changing?

We have been hearing that "data is the new oil" for some time now. With advances in AI, machine learning and CPU processing power, the appetite for data – to mine it, derive insights from it and translate those into new services – shows no sign of abating. Governments, businesses and consumers alike all expect to have more and more information at their disposal, from the personal health tracker to the insurance company's on-board telematics black box.

The Open Banking standard API, released in January 2018, will enable customers to share their account history securely. It is also expected to give rise to new services, such as those that combine banking data with social media or location data, or dashboards on portals where individuals collate all their financial assets in one place. The databases compiled through everyday consumer activity are valuable assets; that much is unlikely to be news to anyone reading this article. A significant advantage can be gained by companies that effectively use this data to differentiate themselves from competitors and offer consumers more relevant products and services.

Technological advances are helping to liberalise the consumer financial services market, and changes such as the Payment Services Directive II next year are also aimed at accelerating this. But the information that fuels this data innovation engine is mainly personal data linked to individuals, and the way this data is handled is set for an overhaul as the EU General Data Protection Regulation (GDPR) comes into effect in May 2018, along with new e-marketing laws. Will the GDPR be a catalyst for innovation or a suppressant? We highlight some of the anticipated impacts of the GDPR.

Personalised offers

Consumers are increasingly able to use soft credit checks and comparison websites to review and make informed choices about the products available to them from a range of suppliers, usually based on the individual's credit score. Companies with access to a customer's account and transaction data, as well as a credit score, can provide tailored offers that more accurately reflect their individual circumstances. At present, the customer's incumbent service provider is likely to have the advantage of holding both sets of data. In the future, with the greater availability of account data, it is anticipated that the field will be broadened to third party providers.

However, with extra data comes extra responsibility. The GDPR regulates all handling of personal data, but it is notable that it identifies 'profiling' for the first time, defining it broadly as any form of automated processing which uses personal data to evaluate certain personal aspects about a natural person, to analyse or predict that person's economic situation, personal preferences, interests, reliability or behaviour activities. Profiling is, therefore, an essential and long-established element of customer acceptance and risk pricing. Contrary to some reports, the GDPR does not ban profiling, but it does make it more challenging. For example:

→ Pre-approving individuals for offers based on their account and transaction data might give rise to a right for that individual to challenge any automated decision made, and demand that it is subject to a human review. The company would be required to take into account the consumer's point of view in this process.

→ Where automated processing does take place, consumers may also have the right to object to the processing of their personal data. This could require the company to either stop using personal data in that way, or demonstrate that it has a legitimate ground on which to process it.

→ Prior to using an individual's personal data, companies must provide transparent, fair processing information, specifying the purposes for which the data is to be used. The GDPR requires that this includes 'meaningful information about the logic involved' in any decision-making.

→ Individuals may have the right to request that their personal data is provided directly by the company to a competitor, as part of the right to data portability.

Marketing channels

Technology offers ever-simpler ways for companies to engage with existing customers. Supplementing web and mobile platforms with targeted offers is a natural step forwards for the financial industry. However, where the offers extended are based on some form of profiling having taken place, companies should consider whether it is necessary to build in the ability to switch offers off for customers on an individual basis. This is a separate consideration to the 'right to object' outlined previously.

As plans for an EU e-Privacy Regulation are finalised, companies may also need to consider the technical methods used to offer these products and services to customers. The revised law promises to significantly increase the scope of communications that fall within the electronic marketing laws and for which consent, or the provision of an opt-out is generally required. Providing customers with these tools may be a time-consuming process.

The big picture

Often management focus is on the headline fines that can be imposed under the GDPR – 4% of annual global turnover or €20m. Yet regulatory sanctions are far from the only cost. Companies should not overlook the opportunity cost of being prevented from extracting full value from their data assets. The importance of data to long-term business strategy will usually justify laying the compliance groundwork today to allow maximisation of data usage tomorrow. Failure to be proactive is inefficient, for example when a raft of consumer complaints highlight essential alterations required by a system, which have to be done in a costly and time-pressured way.

There is uncertainty over the final form of the law (in the case of the e-Privacy Regulation and the national implementation of the GDPR), let alone interpretation or enforcement. Nevertheless, there are tools and measures which can be deployed now to future-proof projects, such as adopting a 'privacy by design and default' policy and carrying out data protection impact assessments. Achieving stakeholder buy-in may be challenging at first, but in the long-run, investment now should pay dividends in the future in the form of maximum flexibility. All sectors are facing considerable challenges; however, the UK financial services industry has been a model for innovation and creativity in the past. There is no reason to suppose that it will not rise to face these new challenges.

Kate Brimsted
Partner, Head of Data and Cyber Security

Tom Evans
Associate, Commercial and Technology

WHY REGULATORS ARE TIGHTENING THE NET ON INITIAL COIN OFFERINGS

The last few years have seen a boom in ICOs, which raise capital funds through issuing cryptocurrency tokens or coins. This innovative fundraising device was initially unregulated, but authorities are waking up to the risks posed by ICOs and beginning to apply regulatory constraints. Matt Baker and Lianna Chan consider the key issues and what we can expect to see from regulators in this fast-moving field.

What is an ICO?

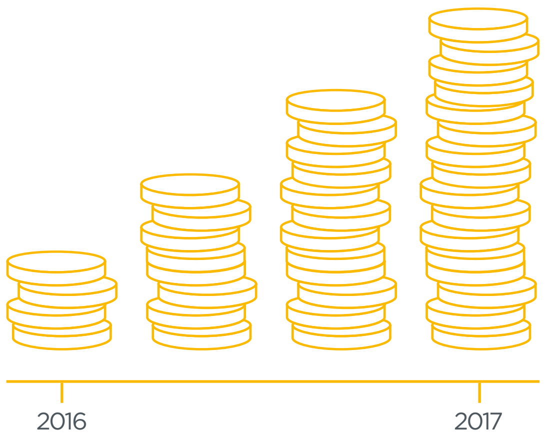
Initial Coin Offerings (ICOs) are a method of public fundraising where a coin or token is issued in exchange for a cryptocurrency/virtual currency (such as Bitcoin or Ether). The coin or token may simply give the right to use the issuer's system or services, or it may offer a share of profits or revenue in the issuer.

Issuers generally produce a white paper describing the key terms of the ICO and providing an overview of the proposed project. But this does not constitute a prospectus, nor does it contain the same amount of information. To subscribe, an investor transfers cryptocurrency to the issuer, and upon completion of the ICO, the coins or tokens will be distributed to the investors which can then be traded on certain exchanges.

ICOs are increasingly popular, particularly among software developers and other technological or disruptive businesses, as substantial funds can be raised quickly from investors worldwide – any individual with internet access can invest. According to CoinSchedule, the number of ICOs more than quadrupled between 2016 and 2017, going from 46 to 211. The highest amount raised by an ICO in this time was $257m (as at mid-November 2017).

Depending upon the features of the particular offering, an ICO may not constitute a security and so less regulation may apply compared to an Initial Public Offering. Whilst that is good news for the issuers, it is beginning to raise concerns with regulators that ICOs may be misused to facilitate fraud or scams.

> "We should expect further significant regulatory developments in this area within the next 12 months"



According to CoinSchedule, the number of ICOs more than quadrupled between 2016 and 2017, going from 46 to 211.

The highest amount raised by an ICO in this time was $257m (as at early mid-November 2017)

Why are ICOs attracting regulatory attention?
ICOs initially had a relatively free rein from regulators, but their increasing prominence means they are coming under growing scrutiny.

Between July and September 2017, risk warnings and statements had been issued by the US Securities and Exchange Commission, and authorities in Singapore, Canada and Hong Kong. China declared ICOs to be illegal and said that all ICOs should 'immediately cease', which was followed by a similar ban in South Korea. In October, the Cypriot regulator, CySec, confirmed it was imposing additional requirements on the firms it regulates when they trade in cryptocurrencies or in CFDs or other derivatives relating to them.

By November 2017, the European Securities and Markets Authority (ESMA) had fired two warning shots on ICOs: One statement warning investors of the risks of ICOs; and another warning firms involved in ICOs of the rules applicable if the ICOs qualify as financial instruments and stressing that "careful consideration" should be given.

ICOs are very high-risk, speculative investments

FCA

What's the FCA's current position?
In the UK, the Financial Conduct Authority warned: "ICOs are very high-risk, speculative investments". It issued a statement warning of the risks associated with ICOs, such as the volatile nature of underlying cryptocurrencies and coins or tokens, and that white papers are not regulated like prospectuses.

Although the FCA accepts that many ICOs will not fall within its scope, it has flagged that each ICO must be assessed on a case-by-case basis. It is not only coin issuers who should consider their position carefully; ICO promoters or trading facilitators may also be caught by the regulatory regime.

In addition to considering whether issuers, arrangers or exchanges should be regulated, the UK's financial promotion regime may mean that coins or tokens that constitute a security cannot be promoted by an unauthorised person, unless the promotion has been approved by an appropriately authorised person.

Furthermore, if a coin or token constitutes a transferable security, the EU Prospectus Directive may apply to the ICO requiring a prospectus to be prepared in compliance with the Directive and approved by a relevant EU regulator unless a relevant exemption applies.

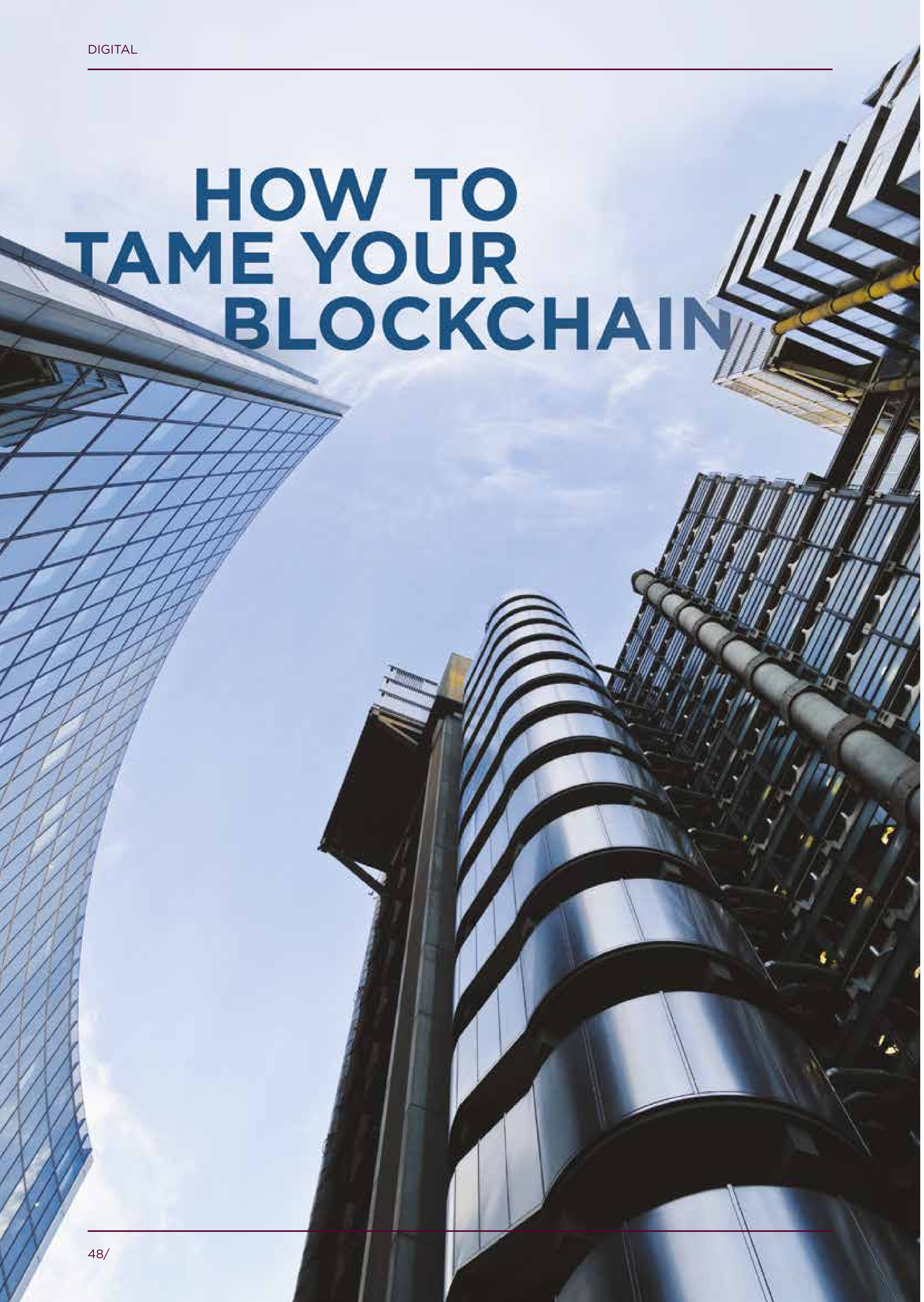
What next for ICO regulation?
In April 2017, the FCA issued a discussion paper looking at the role of distributed ledger technology. In that paper, it sought views from firms on what legal and regulatory challenges there were in the current regulatory framework for ICOs. This represents a potentially significant departure for the FCA, which previously sought to be technology-neutral in the way it regulates. The FCA is currently considering the responses and is expected to publish its findings soon.

In the meantime, the FCA has already issued a further statement on cryptocurrencies but in relation to cryptocurrency CFDs, making it clear that firms offering such CFDs must be authorised and supervised by the FCA; as well as warning consumers that the value of cryptocurrencies and the CFDs linked to them is "extremely volatile".

Given the increased commentary and scrutiny from international regulators, and the divergence in approaches being taken, we think that it is more crucial than ever for issuers, promoters and any other parties involved in an ICO to obtain robust regulatory advice from all relevant jurisdictions. We should expect further significant regulatory developments in this area within the next 12 months, including potentially seeing regulators coming down harshly on any ICOs that misjudge, or failed to consider, whether they fall within the regulatory scope.

Lianna Chan
Associate, Financial Services Investigations

Matthew Baker
Partner, Investment Management



HOW TO TAME YOUR BLOCKCHAIN

Blockchain has been heralded as a game-changer for the insurance industry, a distributed ledger technology (DLT) that can improve processes, reduce error and address fraud. In 2018, a new initiative between AP Moller-Maersk, EY, Microsoft and certain insurers will use DLT in a marine insurance platform. Usman Wahid looks at the opportunities offered by this technology – and the governance challenges it poses.

A technology with transformational potential

DLT has particular potential in the insurance sector as it can make multi-party, multi-jurisdictional business processes more efficient by removing any duplication in data-entry and reconciliation, and automating certain transactions (through smart contracts).

For example, smart contracts recorded on blockchain could deal with and pay claims automatically when certain conditions (whether assessed from publically available information such as flight delays, or from devices with 'Internet of Things' capabilities such as home sensors) are met, without any need for further assessment.

If claims are also recorded, DLT could reject cases where multiple claims for one incident are submitted, helping to reduce insurance fraud. Claims that need further processing could also be made more efficient as brokers, insurers and reinsurers could all view changes to the data at the same time.

The choice between public and private blockchains

The issue that we feel of key importance to potential insurance sector users of DLT will be that of governance. The insurance sector is unlikely to use public blockchain technologies, such as Bitcoin and Ethereum, because anyone can participate in them; the security of public blockchains depends on everyone seeing and storing each transaction. This not only gives rise to confidentiality issues, but also issues of immutability – it is almost impossible to reverse blockchain transactions once a sufficient level of validation is reached.

The more likely take-up by the insurance sector will be in private blockchains as their governance can be structured in a more business appropriate manner. For example, unlike public blockchains, a private blockchain can be managed by the technology company behind the blockchain or there can be an agreed set of rules for dealing with governance issues.

These governance issues include whether a new party can participate in the DLT system (e.g. introducing a reinsurer in a claims accounting system) and when to reverse transactions (e.g. if facts are disclosed late which indicate a claim was fraudulent).

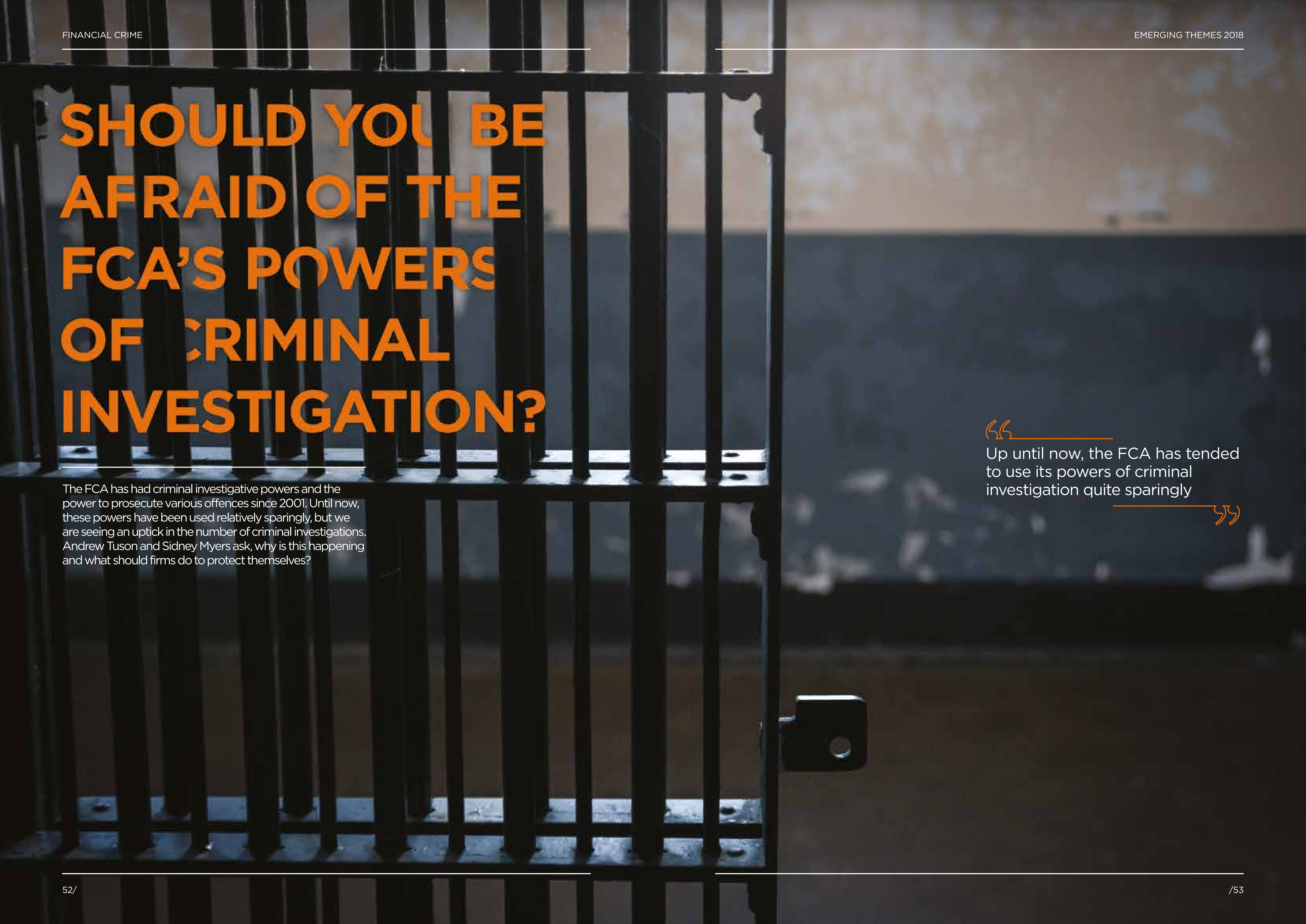
Designing governance structures

There are various ways to structure the rules governing how these decisions should be made. One particular DLT technology company uses a mining diversity technique which requires a minimum proportion of the permitted participants to participate in order to create a valid decision, much like a quorum requirement for board meetings. Private blockchains are also more easily editable, should a transaction need to be reversed.

In the insurance sector, rules-based governance agreements will therefore need to be agreed by participating parties to ensure that decisions are made on an equal and fair basis. Without such rules, the proposed benefits of DLT could be compromised.

Usman Wahid
Partner, TMT, Commercial & Technology, Outsourcing

Financial CRIME



SHOULD YOU BE AFRAID OF THE FCA'S POWERS OF CRIMINAL INVESTIGATION?

The FCA has had criminal investigative powers and the power to prosecute various offences since 2001. Until now, these powers have been used relatively sparingly, but we are seeing an uptick in the number of criminal investigations. Andrew Tuson and Sidney Myers ask, why is this happening and what should firms do to protect themselves?

> "Up until now, the FCA has tended to use its powers of criminal investigation quite sparingly"

Why the FCA is making greater use of its powers
"Be afraid, be very afraid" the former CEO of the FSA, Sir Hector Sants, famously warned would-be insider dealers and anyone tempted to engage in market abuse. In contrast, Mark Steward, the FCA's current Director of Enforcement and Market Oversight prefers to speak softly and carry a big stick. His mantra is that his department needs to "cover the waterfront", meaning there should not be any no-go areas for the Enforcement Division, and no parts of the industry should be immune from regulatory scrutiny and enforcement.

Despite this seemingly more benign philosophy, we have started to detect a significant change in the FCA's approach to its statutory powers, nowhere more so than the regulator's powers of criminal investigation. Such powers are not new – they are to be found in the Financial Services & Markets Act 2000 – but, up until now, the FCA has tended to use them quite sparingly. We think that could be starting to change in at least two key areas, namely anti-money laundering compliance and market abuse.

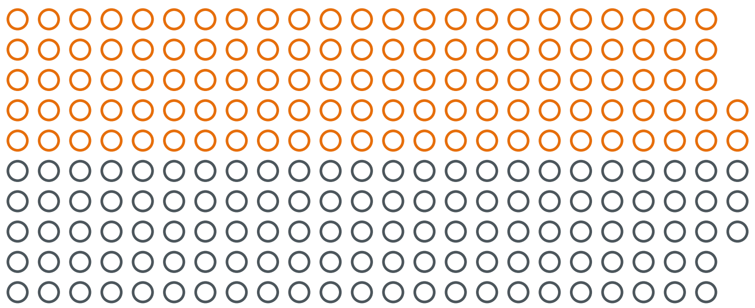
In recent months, we have begun to detect a greater willingness on the part of the FCA to commence 'dual track' regulatory/criminal investigations when looking into suspected breaches of the Money Laundering Regulations. Indeed, this new approach was foreshadowed in the FCA's 2017/18 Business Plan, which notes that "where firms have poor AML controls, we will use our enforcement powers... if failings are particularly serious or repeated, we may use our criminal powers to prosecute firms or individuals."

> "The FCA appears to be taking a much more rigorous approach to their conduct of criminal investigations than in prior years"

Money Laundering Regulations 2017: Do you have the right measures in place?
There is some inconsistency in the approach taken by the FCA where it suspects breaches of the Money Laundering Regulations, ranging from giving firms additional time to remediate through to commencing parallel regulatory and criminal investigations. Given the seriousness of the action which the FCA can take, it is important that firms have properly addressed their obligations under the new Money Laundering Regulations 2017. This includes ensuring that they have appropriate policies and procedures in place and appropriate training programmes, focusing on the specific risks faced by their businesses.

Where the FCA investigates firms under the Money Laundering Regulations, it also examines whether a criminal investigation should be opened against a member of senior management whom the FCA considers may be involved in the firm committing a criminal offence, or where the corporate liability may be attributed to any neglect on the part of the individual officer. This is becoming a significant risk, as criminal charges can be brought against individuals even where no fraudulent conduct is suspected. A criminal case can be brought simply for compliance failings.

A parallel shift in approach can be detected in relation to market abuse. Emboldened by its strong track-record of prosecuting insider dealing offences, the FCA is now looking to use its powers to investigate and prosecute other forms of market misconduct (such as market manipulation) which may, in the past, have been dealt with under the civil market abuse regime. Mark Steward has made clear that, given Parliament has determined that market abuse is a criminal offence, the public expects the FCA to conduct criminal investigations and use these powers, only falling back on the civil regime where there is insufficient evidence for a criminal prosecution. The FCA's 2016/2017 annual report stated that 235 new enforcement investigations were opened in 2016/2017 (excluding unauthorised business and applications to revoke or vary permissions). Nearly half of these investigations related to market abuse, mostly insider dealing.



OF THE 235 NEW ENFORCEMENT INVESTIGATIONS CONDUCTED BY THE FCA NEARLY HALF WERE RELATED TO MARKET ABUSE

Take action now to ensure compliance
Given the potential exposure in relation to market abuse investigations, firms should ensure they are fully compliant with the Market Abuse Regulation and that they have appropriate systems and controls in place to prevent market abuse from occurring in their businesses. Moreover, firms also need to ensure that any suspicious orders and transactions are escalated so that Suspicious Transaction and Order Reports can be filed as appropriate. Taking such action now should help to demonstrate that firms are appropriately committed to complying with their regulatory responsibilities and help to protect firms from criminal and civil market abuse investigations.

In practice, where the FCA undertakes hybrid civil and criminal investigations it appears to be taking a much more rigorous approach to conduct of criminal investigations than in prior years. In particular, the FCA Enforcement and Market Oversight Division increasingly declines to invite firms to attend scoping meetings for hybrid investigations, instead seeking to conduct interviews under caution in compliance with the Police and Criminal Evidence Act. In the past, the FCA often investigated as if they were only conducting a civil regulatory investigation, including holding scoping meetings and conducting compelled interviews.

54

LIVE CRIMINAL INVESTIGATIONS ARE UNDERWAY BY THE FCA

The approach now adopted in these 'dual track' investigations is somewhat at odds with the changes to the approach to enforcement investigations generally, following the Green Report, in that the Enforcement Division now tends to be much more communicative and open about the status and progress of its investigations.

A recent Freedom of Information Act request revealed the FCA had 54 live criminal investigations. Given the FCA's much tougher approach towards potential breaches of the criminal law, it would seem that not only insider dealers and professional fraudsters need to be afraid.

Sidney Myers
Consultant, Financial Regulation

Andrew Tuson
Partner, Commercial Dispute Resolution

TECHNOLOGY AND THE FIGHT AGAINST FINANCIAL CRIME:

IS THERE MORE THAN MEETS THE EYE?

Increased use of technologies such as digital payment systems has created new targets for criminals, but new solutions are also being developed to detect and prevent financial crimes, such as money laundering. Clare Reeve looks at whether automated AML systems are likely to enter the mainstream, and the FCA's role in the adoption of these technologies.

IT and communication technologies are essential to the functioning of the economy and, inevitably, these rapidly evolving technologies have become a prime target for criminals as cyber-attacks are now an everyday occurrence. The ongoing development of cryptocurrencies and digital delivery channels presents fresh challenges for businesses, regulators and law enforcement agencies. The astonishing change of pace makes it difficult for the authorities to keep up.

The implementation of the EU's Fourth Money Laundering Directive and enactment of the Criminal Finances Act brought financial crime into sharp focus in 2017 and Anti-Money Laundering (AML) remains a priority for the FCA. In response to increasing legislation and regulation, the number of financial crime-related compliance professionals and lawyers working in banks and regulated firms has increased considerably in recent years. The introduction of new technologies and digital delivery channels and systems into regulated firms can only increase the already considerable workload of compliance teams. On the flip-side, however, new digital solutions and technologies are also being developed with a view to making AML compliance systems and controls more efficient.

> Balanced against the potential benefits of automated AML technology are privacy and security concerns

Emerging technologies to assist AML compliance

Many regulated firms, including several retail banks, are already using fingerprint, voice and/or other biometrics to tackle customer identity fraud. Transaction monitoring is another area which is heavily technology-driven.

Increased automation and technologies, such as machine learning and data analytics, are likely to benefit areas of AML compliance, including customer due diligence and transaction monitoring.

As with predictive coding – a type of machine learning that is used to aid the process of litigation disclosure – it is easy to envisage the use of technology that not only identifies and flags relevant information from different sources, but summarises high-risk issues potentially more effectively and efficiently than current human-based systems. This would reduce false positives and their costs.

Balanced against the potential benefits of using new technologies are privacy and security concerns. Along with the significant investment that would likely be required, these issues will be important factors in firms' decisions on whether to update their systems and controls using new technologies. In addition, there are certain areas of AML compliance where the use of new technologies is likely to be more limited, for example suspicious activity reporting under the Proceeds of Crime Act 2002 (POCA) where it is difficult to envisage a successful process of disclosure and reporting being adopted by firms without significant human input and oversight.

Is the FCA a driver of innovation?

Since the launch of Project Innovate in 2014, the FCA has been focused on increasing competition through innovation. The so-called regulatory sandbox was introduced by the FCA as a 'safe space' to test new technologies, products and services and receive the FCA's feedback without fear of enforcement action, provided firms comply with agreed testing and reporting parameters. The third cohort began testing in November 2017 and included at least three firms testing AML compliance-related technologies, such as artificial intelligence-driven transaction monitoring systems.

In August 2017, the FCA published a report that it had commissioned into the application of new technologies in AML compliance, which involved three months of research and over 40 interviews with regulated firms, technology providers and other bodies.

Industry-wide utilities, which effectively outsource various compliance activities such as due diligence are used by many institutions. These were considered one of the most attractive areas for development given the likely cost efficiencies and the ability to identify issues and trends more easily from a bigger data set.

The report concluded that new and emerging technologies, including those related to client onboarding/due diligence and transaction monitoring, have genuine potential to have a transformative impact on AML compliance. This conclusion was echoed in a recent speech by the FCA's Head of Financial Crime, Rob Gruppetta. In the context of artificial intelligence, Mr Gruppetta agreed that new technologies have the capability to assist AML compliance, but noted that it will be a constant work in progress.

> An FCA report published in August 2017 concluded that new and emerging technologies, including those related to client onboarding/due diligence and transaction monitoring, have genuine potential to have a transformative impact on AML compliance

Clare Reeve
Senior Associate,
Commercial Dispute Resolution

AML compliance in the future

Whilst new technologies have the potential to bring about more efficient and perhaps more effective AML processes, it is difficult to predict to what extent regulated firms will embrace new technologies and how AML compliance systems and controls will change over the coming years. Disincentives include the cost of investment, data protection concerns and potential implications of failure for individual compliance officers and/or senior management.

Perhaps we will see a shift in recruitment strategy for AML compliance staff, particularly amongst the larger firms and institutions looking to strengthen their AML technology expertise. However, any significant change or displacement of current approach to AML compliance is likely to struggle to gain proper traction unless there is commitment on a market-wide basis, including support from the relevant regulators.

The message communicated in the FCA's AML technology report was that views were generally positive about the FCA as a front runner in AML innovation, but further action would be welcomed. Mr Gruppetta, in his December speech, acknowledged that the FCA need to do more thinking on the adoption and implementation of new technologies. This should include the facilitation of industry-wide discussions on AML compliance and the introduction of new regulations and guidance or updated rules to reflect the emergence of new technologies. Technology has the potential to transform AML compliance if the FCA and the industry can overcome the current obstacles to progress.

INVESTIGATIONS

PRIVILEGE AFTER ENRC – WHY THE PRA AND FCA ARE ALSO FEELING THE PAIN

> Exchanges between the enforcement team and external or internal experts on the issues under investigation are unlikely to be protected by legal privilege

Over the last few months many column inches have been filled with lawyers complaining about the unsatisfactory state of the law of privilege in the context of regulatory investigations, following the recent decision in The Directors of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd [2017] EWHC 1017.

Yet the decision equally creates problems for regulators – and opportunities for defence counsel – in the context of documents created by the regulator in conducting its investigation.

Unless the judgment is reversed on appeal, various categories of documents created by lawyers in the course of a regulatory and/or criminal investigation are unlikely to attract legal advice privilege or litigation privilege under English law.

As well as applying a narrow construction to the issue of who constitutes "the client" for the purpose of legal advice privilege when internal interviews are conducted, the Court also adopted a restrictive approach to the issue of the point from which litigation is treated as being in "reasonable contemplation" for the purpose of litigation privilege, in the context of an investigation. This aspect of the ENRC decision is likely to be as unwelcome to enforcement teams at the PRA and FCA as it is to those representing firms and individuals suspected of breaching regulatory rules.

The Court determined that a criminal investigation is not itself adversarial litigation for the purpose of the test for litigation privilege. The same must be true of a regulatory investigation. Accordingly, documents created for the dominant purpose of use in the investigation – for example, communications between the firm's lawyers and their experts for the purpose of persuading the regulator to discontinue its investigation - will not attract litigation privilege.

Perhaps more surprisingly, the Court also identified that the fact that a defendant is under criminal investigation does not in itself create a likelihood that a prosecution will follow. It is only once a prosecution becomes a real prospect for the defendant that litigation privilege will begin to apply. The Court held that a prosecution only becomes a real prospect for a defendant once it is discovered that there is some truth to the allegations, or at the very least that there is some material to support the allegations of (in this case) corrupt practices. This will be a question of fact in every case.

The evidential threshold for the PRA and FCA to commence a regulatory investigation is a low one – simply that there are circumstances suggesting that a breach may have occurred, or that an individual may not be fit and proper. As the PRA and FCA are at pains to make clear when an investigation is commenced, they have not yet reached any view and have an open mind as to whether or not any breach has occurred.

THE PRA AND FCA CAN BE PRESSED FOR DISCLOSURE OF NON-PRIVILEGED COMMUNICATIONS AT THREE STAGES:

1. As part of settlement negotiations when annotated draft warning notices and accompanying documents are disclosed.

2. Following issuance of a warning notice when the regulators are required to disclose documents which might undermine their case under Section 394 FSMA.

3. Following a referral to the Upper Tribunal for an independent hearing when a full disclosure exercise is followed.

What does the future hold?

It will be difficult for the PRA or FCA to assert privilege over any communications created in the course of their investigation, at any stage prior to an internal determination that a breach has been committed - except where they are between a lawyer and their client for the purpose of giving or receiving legal advice (or as part of that continuum of communications). As a result, any communications between the enforcement team and supervisors, or exchanges between the enforcement team and internal or external experts on the issues under investigation, or communications between the enforcement team and senior management at the regulators, are unlikely to be protected by legal privilege.

As a result in the year ahead I expect that we will see increased levels of challenge of claims to legal privilege, both from the regulators on firms and individuals under investigation but also by those subjects of an investigation seeking greater access to the regulators' own sensitive communications.

> It will be difficult for the PRA or FCA to assert privilege over any communications created in the course of their investigation, at any stage prior to an internal determination that a breach has been committed

Nathan Willmott
Partner, Head of Financial Regulation

PIERCING PRIVILEGE: REGULATORY INVESTIGATIONS IN THE DUBAI INTERNATIONAL FINANCIAL CENTRE

In some ways the DFSA resembles its UK counterpart, the FCA. But beware, the rules on document disclosure and legal privilege under the DFSA are very different. Raza Mithani and Kate Pooler explain key rules you need to know about if you operate in the DIFC.

The Dubai Financial Services Authority (DFSA) is the independent regulator of financial services conducted in or from the Dubai International Financial Centre (DIFC), a purpose-built financial free-zone in Dubai. The DIFC is a common law and English language jurisdiction. In circumstances where DIFC legislation does not address a matter at hand, the DIFC courts look to English law as providing the ultimate backstop.

On that basis one might assume that the DFSA has similar powers of supervision, investigation and enforcement to the FCA, and that the normal rules of legal professional privilege apply to information that is of interest to the DFSA in its investigations. Whilst the first assumption has a sound foundation, the second would be mistaken.

Legal privilege for FCA regulated firms

FCA regulated firms are not required to produce or disclose to the FCA communications made between client and lawyer that are made in connection with the giving of legal advice to the client. The statutory protection under section 413 of the Financial Services and Markets Act exists in addition to the common law protection. That section provides that a firm cannot be required by a regulator to produce or disclose a 'protected item'; 'protected items' include communications between lawyer and client (or any person representing the client) which is made in connection with the giving of legal advice.

How privilege differs under the DFSA Rules

Where the DFSA has made a request for specific documents; confiscated documents pursuant to a without-notice search of business premises; or required an individual to attend a compulsory interview, a firm or individual cannot refuse to comply with the DFSA on the grounds that a disclosure may serve to (a) incriminate them or (b) reveal a communication attracting legal professional privilege.

> The default position is that proceedings of the Financial Markets Tribunal are public

Lawyers may refuse a request on grounds of privilege, but must then promptly provide the DFSA with a written notice disclosing the name and address of parties to the communication (if known), and sufficient particulars to identify the document containing the communication. Armed with that information, the DFSA can simply present the relevant firm or individual with a request for the specific document.

In the normal conduct of an investigation by the DFSA, any information unearthed pursuant to its investigation remains confidential and, should that information later be relevant to any civil proceedings, remains subject to that court's normal rules on admissibility. This means that the privileged nature of communications that have been disclosed in DFSA investigations may be restored in the context of certain court proceedings.

If, however, the communication becomes the subject of a referral or relevant to proceedings in front of the Financial Markets Tribunal (FMT) of the DFSA, the rules are very different. The FMT reviews DFSA decisions and hears proceedings brought by the DFSA or by any other person whose claim has received DFSA consent.

Why you risk losing privilege if you come before the FMT

In determining a proceeding, the FMT may receive and consider any evidence (oral or written) even if such evidence may not be admissible in civil or criminal proceedings in a court of law. Further, the default position is that proceedings of the FMT are public. An FMT order declaring that this would "significantly harm…[a party's] business interests" must be obtained in order for the hearing to be held privately.

Herein lies the danger: the DFSA may have obtained privileged communications pursuant to an investigation because the defence of privilege can only be raised by a lawyer. The DFSA delivers a confidential decision that is then referred to the FMT for review. The privileged communications that would normally not be admissible in a court of law are admissible before the FMT and are put to the tribunal in a public hearing. Consequently, the communications may thereafter not be considered privileged by any court of law because those communications have now entered the public domain and only confidential communications are privileged.

Certainly under English law "once [information] has entered what is usually called the public domain…the principle of confidentiality can have no application to it" *(Attorney-General v Guardian Newspapers Ltd (No. 2)* [1990] 1AC 109).

A Singaporean case earlier this year diverged from that position in finding that the principle of confidentiality underpinning privilege could still protect information that had been made available on WikiLeaks (*Wee Shuo Woon v HT S.R.L.* [2017] SGCA 23). The extent to which the information had in fact been accessed by the general public was stressed, as was the equity in offering protection to information leaked as a result of an unlawful cyber-attack. This equity is harder to apply to information that had been put in the public domain on account of a lawful investigation by a regulator.

Firms that deal with DFSA regulated entities need to be mindful of this potential route around legal professional privilege, and understand the difference in approach adopted by the DIFC regulator.

> A firm or individual cannot refuse to comply with the DFSA on the grounds that a disclosure may serve to (a) incriminate them or (b) reveal a communication attracting legal professional privilege

CHALLENGING THE DFSA CAN RESULT IN LOST PRIVILEGE

1. The DFSA obtains privileged communications in an investigation.
2. DFSA delivers a confidential decision.
3. The decision is referred to the FMT for review.
4. Privileged communications are put to the tribunal in a public hearing.

Raza Mithani
Partner,
Commercial
Dispute
Resolution

Kate Pooler
Trainee Solicitor,
Commercial
Dispute
Resolution

The number of high profile regulatory investigations is on the increase, along with investigations into trading irregularities. When the authorities come calling, it is vital to be able to find key, relevant documents effectively and efficiently. Paul Bennett considers the best strategy for managing the search for documents.

Why manual searches are not the answer

Given the volume and range of electronic data that will inevitably be collected in such investigations, it is highly unlikely that it will be possible for lawyers to review every single document, even after de-duplication. The challenge is therefore to find the right approach and technology that will best assist with the specific requirements of each review exercise. There are a number of strategic approaches that could be taken for a large document review exercise:

1. Keywords

A tried and tested approach is to use keywords to cull data down to a volume of documents that can be reviewed by a team of paralegals and lawyers. One advantage of this approach is that it may well identify the majority of documents that relate to the issues on which the keywords have been based.

However, this approach will not identify all documents and, perhaps more importantly, it will not identify any documents that relate to issues that are not known about at the time the keywords are chosen. This keyword-based approach can be less effective to investigate situations of alleged wrongdoing, especially where the perpetrators are likely to have disguised their activities through the use of code words or non-standard language.

From a Forensic Technology perspective, the use of keywords can feel like a very blunt tool.

2. Analytics

Analytics is a far more sophisticated tool that comprises concept clustering, email threading and a 'find similar documents' function, among other capabilities and techniques. This can dramatically improve the speed with which key relevant documents are identified, or unknown issues uncovered, which can be extremely powerful and of real value to an investigatory team.

Visual analytics is a highly effective way for a client or legal team to understand the data that has been collected at an early stage in an investigation. With this enhanced knowledge, the planning and focus of a workflow can be suitably prioritised to ensure the most effective document review exercise is undertaken – in terms of both cost and finding the 'hot docs'.

3. Predictive coding

This is another useful tool for prioritising document review. At its simplest, predictive coding could involve reviewing a sample document set, after which all remaining documents in the population can be ranked in order of those most likely to be relevant. As the document review continues, the system is continually updating or 'learning'. The review approach could be to focus on those documents that are categorised by the software as being most likely to be relevant.

One of the many advantages of predictive coding is the fact that it produces a workflow that is completely repeatable and defensible to regulators or any other party with a vested interest.

It is clear there is no one-size-fits-all approach to any regulatory investigation. The important thing is to make sure you have all the technological tools at your disposal to give you the best opportunity to find the key documents in the most effective and efficient manner.

> Given the volume and range of electronic data that will inevitably be collected in such investigations, it is highly unlikely that it will be possible for lawyers to review every single document

Paul Bennett
Partner, Head of Forensic Services

TAX EVASION REMAINS HIGH ON THE POLITICAL AGENDA

Tax avoidance and tax evasion continue to be hot topics, and HMRC is stepping up its efforts to maximise compliance and target offenders. New offences under the Criminal Finances Act 2017 have recently come into force, criminalising corporates that fail to prevent the facilitation of tax evasion. Kate Ison sets out the key themes we can expect to see in the tax environment in 2018.

Tax is now a regular front page issue in the UK media, whether it's a story about tax avoidance, tax evasion or more generally the tax affairs of businesses operating in this country.

Amid this increased focus on tax, the lines between legal tax avoidance and illegal tax evasion have become blurred. Avoiding tax is generally lawful, even if schemes often prove to be ineffectual. Evasion of tax is generally illegal and involves dishonesty and concealment. The common mantra is that everybody should pay their fair share of taxes and in this environment, for reputational reasons alone, it is vitally important that corporates are seen to be compliant with tax law.

The UK tax authority (HMRC) has appeared to welcome the increasing focus on tax because it hopes to increase revenues and change corporates' behaviour. On 20 July 2017, HMRC published its business plan for the next three years and its key strategic objectives for this period. At the top of the list is HMRC's objective to maximise revenues due, and bear down on avoidance and evasion. To achieve this, the Government has committed to investing £800m into additional work led by HMRC to counter tax avoidance and tax evasion.

In this changing tax environment, we can expect to see some of the following themes emerge in 2018:

1. **Changes to risk profiling of corporates:** HMRC is rolling out a series of measures focusing on taxpayer behaviour and designed to promote tax compliance. This includes the requirements for large businesses to publish their strategy on tax, including how they manage tax risk and their appetite for tax planning. HMRC is also consulting on proposed changes to risk profiling of corporates, the outcome of which is the likely impact on how taxpayers engage with HMRC on a real time basis, and the degree of scrutiny to which their affairs are subject.

2. **An increase in civil enquiries:** HMRC is expected to continue its current trend of opening an increased number of enquiries into self-assessments, challenging historic structures and labelling tax planning as aggressive, in order to meet its objective of yielding maximum revenues.

3. **More information requests:** following a steady creep of legislative changes, HMRC now has very wide information-gathering powers, which it is employing ever more frequently. In particular, in recent months HMRC has issued broad and extensive information requests to a number of third parties – very often banks – compelling the provision of information which the third party holds in relation to its dealings with another taxpayer. This trend is expected to continue in 2018.

4. **Investigations being initiated under the Criminal Finances Act:** the Government has set HMRC high targets to increase the number of criminal investigations which it undertakes, with a view to increasing the number of criminal prosecutions in relation to tax crime to 100 by the end of this Parliament. In the past, HMRC has been criticised for investigating small businesses for low value crimes, which have been viewed as a 'low hanging fruit', in order to meet its targets. It is expected that HMRC's attention will now turn to financial institutions and large corporates to counter this criticism. One immediate focus area for HMRC will be investigation of suspected criminal offences introduced by the Criminal Finances Act 2017, which applies to corporates that have failed to prevent the facilitation of tax evasion. Corporates operating in the financial services sector are likely to be closely scrutinised.

5. **Civil penalties for enablers of defeated tax avoidance arrangements:** new rules introduced in late 2017 empower HMRC to impose civil penalties on so-called enablers of abusive tax arrangements which are later defeated in court or settled. Banks will fall into the category of 'enablers' where they provide financial products, including loans, shares or derivative contracts, where they know that one of the purposes of obtaining the product is to be used in abusive tax arrangements. Financial institutions which adopt and comply with the Code of Practice on Taxation for Banks are unlikely to fall foul of the new enablers regime. However, they should now review their existing code of governance to ensure that it is sufficiently robust to protect against the risk of an "enablers" penalty being imposed.

Kate Ison
Senior Associate,
Corporate Tax

INDIVIDUAL *Accountability*

SMCR – PROTECTING YOUR MIDDLE MANAGERS

The new Senior Managers and Certification Regime will be extended to all authorised firms throughout 2018 and 2019. Polly James and Joseph Ninan offer practical tips on the implications for middle managers. What are the unexpected consequences hidden in the small print, and how can you manage personal regulatory risk effectively?

> Under the extended SMCR, all individuals except for pure administrators will be subject to personal regulatory duties under COCON Individual Conduct Rules 1–5

We often defend senior individuals in regulatory enforcement proceedings. The driving force behind the Senior Managers and Certification Regime (SMCR) is a desire to make it easier to fine and ban individuals when regulatory breaches happen within firms. As defence practitioners, we must understand exactly how the new rules change things in practice, to ensure we can continue to provide both the most effective practical tips on how to minimise personal regulatory risk in the first place, as well as the best strategic advice on defending the position when somebody finds themselves subject to an enforcement investigation.

Here, we'd like to share some unexpected consequences of the SMCR for middle managers and explain what individuals need to do to protect themselves from personal regulatory exposure.

OUR TOP TIPS

1. Understand your personal responsibility – having a difficult boss doesn't take COCON duties away.
2. If you are a Senior Manager, ensure your Statement of Responsibilities is always up to date.
3. Make a written note of reasons for decisions – don't expect regulators to take your word for it.

Reading between the lines of the new rules – bad news for middle managers

The FCA has slipped some particularly onerous new regulatory duties into the new rules for people who are not senior enough to fall within the fairly limited "SMF" (Senior Management Function) population, but who nonetheless have responsibility for managing others.

Under the current Approved Persons regime, individuals who are carrying out Controlled Functions (e.g. CF30, Customer Function) that are not Significant Influence Functions (SIF) do not owe any regulatory duties in respect of their management of others. Their regulatory duties are simply to act with honesty and integrity, with due skill, care and diligence, observing proper standards of market conduct, and to deal with regulators in an open and cooperative way, disclosing to the regulators 'any information of which [a regulator] would reasonably expect notice'.

By contrast, under the extended SMCR, all individuals (except for pure administrators) will be subject to personal regulatory duties under COCON Individual Conduct Rules 1–5. These duties go far beyond the previous duties under APER in respect of managing others.

The new guidance in the FCA Handbook at COCON 4 takes the managerial regulatory duties that, under APER, only apply to the SIF holders, and applies those standards to everyone whose responsibilities include managing others. It does this by including, as guidance to the Individual Conduct Rule 2 duty to 'act with due skill, care and diligence', statements that were previously only relevant to SIFs such as: 'Where explanations [given to a manager] are implausible or unsatisfactory, they should take steps to test the veracity of those explanations.'

The FCA has quite deliberately attached regulatory consequences to matters that, in the old world, would have been purely questions of management competence. As a result they have given themselves greater opportunity to bring enforcement action against middle managers in respect of the quality of their management, an area that was previously out of the FCA's reach.

> The FCA is quite deliberately attaching regulatory consequences to matters that, in the old world, would have been purely questions of management competence

Prevention is less painful than defence

Nobody wants a PRA or FCA Notice of Appointment of Investigators to land on their desk, or to see this happen to anybody in their team. To minimise the risk of personal regulatory exposure under the new regime, here are our top tips:

1. If you manage others, make sure you understand the scope of the new regulatory duties that the FCA is about to impose upon you as a manager. These look quite different to the scope of the duties you are used to.
2. Even if you are not currently an Approved Person, you are about to take on personal regulatory duties under the Individual Conduct Rules in COCON. As a result, you must ensure you understand these duties properly, own your decision-making and recognise that (for example) having a difficult boss doesn't take your COCON duties away.
3. If you are a Senior Manager, make sure your Statement of Responsibilities (the document that defines the scope of your role for regulatory purposes) is always up to date – if not, you risk having regulatory duties that you cannot fulfil.
4. If you haven't documented it, you haven't done it. The regulators often refuse to believe something happened unless it was documented. This doesn't have to mean formal meeting notes and defensive email trails that will burn you out and make you unpopular – you could simply keep a handwritten daybook to record each key decision that you make, together with reasons for making it. You may not remember these reasons for the six years, or even longer in respect of a prohibition action, that the regulators now have to commence an enforcement action against you.

When you have no choice but to enter defence mode

There are multiple changes afoot within the FCA Enforcement Division (and changes are expected within the PRA's Regulatory Action Division, which is further behind in its response to the Treasury's Enforcement Process Review). These changes include:

→ A new policy of encouraging investigators to take on cases with a completely open mind, rather than focusing on securing a particular outcome.

→ The introduction of internal case management meetings on a four – six weekly basis.

→ More frequent communication between the FCA and the individual under investigation.

The upshot of this is that it is more important than ever to frontload your work on the defence position, and (provided that there are no allegations of criminal misconduct by the FCA) be proactive in putting forward your position to the regulator, with a view to securing an early discontinuance.

We are in the process of putting together an SMCR implementation toolkit, to help you deal with the practical challenges of implementing SMCR and covering your compliance, HR and record-keeping policies and procedures. Please speak to your usual BLP contact if you would like to know more.

Polly James
Partner,
Financial Services Investigations

Joseph Ninan
Associate,
Financial Services Investigations

EMPLOYEE MISCONDUCT

NAVIGATING THE WEB OF REGULATORY AND EMPLOYMENT LAW DUTIES UNDER SMCR

Disciplinaries against Senior Managers and Certification Staff trigger both regulatory and employment law duties. The extent of these duties depends on the nature of the alleged misconduct. Are we dealing with a breach of the Conduct Rules? Is the alleged misbehaviour sufficient to call into question the employee's fitness and propriety? Do we need to tell the regulator?

Let's imagine a familiar scenario, where an employee (who is a Senior Manager or Certification Staff member) breaches their confidentiality obligations by sending confidential information, including sensitive customer information, to a personal email address. What do you do on discovering the breach?

Will you suspend pending the disciplinary investigation?
From an employment law perspective you need reasonable grounds to suspend. If there's a risk that the employee will interfere with evidence or tamper with witnesses then this would suffice. Further considerations are relevant under the Senior Managers and Certification Regime (SMCR). Given the alleged conduct may amount to a serious breach of the Conduct Rules, and go to the heart of the assessment of the individual's fitness and propriety, it may not be appropriate for the employee to continue in their role until the breaches have been fully investigated and the prospect of further breaches has been ruled out. You could consider whether it is reasonable to move the employee to another part of the business while the investigation is ongoing, although in practice the seniority of the employee may make this highly impracticable.

Do you have temporary cover lined up?
While suspended, you will need someone to step into the Senior Manager or Certification role on a temporary basis.

If it is a certification function and the suspension will last longer than four weeks, then the employee covering will need to be certified.

If it is a Senior Manager role and the suspension will last longer than 12 weeks, you will need to apply to the regulator for pre-approval. If pre-approval is needed, or the employee needs to be certified, then you will need to comply with your obligations to obtain regulatory references going back six years.

A living handover document is key in this scenario. If one does not exist, then use the opportunity to obtain a handover while the employee is suspended, particularly if faced with a potential non-amicable termination later down the line.

Are they fit and proper?
This confidentiality breach may impact on the assessment of the employee's integrity, particularly if it was a deliberate act, and/or competence and capability, both of which are key factors when determining fitness and propriety.

If the employee is suspended, the question of their fitness and propriety is only likely to actively arise if you are in the process of undertaking the annual certification process in respect of Certification Staff (for example, as part of the appraisal process). In such circumstances, it is unlikely that the line manager will feel comfortable certifying that the individual is fit and proper, and the renewal of the certificate may need to be delayed until after the internal investigation and/or suspension period ends.

What if the employee resigns before the process is concluded?
Should you continue with the disciplinary process based on the information you have? If the resignation is on notice, rather than allegations of constructive dismissal, you can instruct the employee to continue to take part in the process – although they may be prevented from doing so through stress-related absence.

There are two good reasons for continuing with the investigation:

1. The Senior Manager responsible for that area may want comfort that there are no outstanding regulatory issues within their area of responsibility. For example, have we got to the root of the issue, is anyone else involved, or are there any systems or controls that require improvement?

2. You will need to provide information in any subsequent regulatory reference that you reasonably consider to be material to the assessment of whether the individual is fit and proper – the allegations made and any conclusions reached as part of the disciplinary process (even if no formal disciplinary action is taken as the employee has resigned) may need to be included in the reference.

Catherine Turner
Senior Associate,
Employment

Adam Jamieson
Senior Associate,
Financial Services
Investigations

Are there any settlement agreement considerations?
If you do end up parting ways and entering into a settlement agreement, there are two key points to consider:

1. Ensure the employee agrees to a full handover as part of the termination terms.

2. Ensure you do not compromise your regulatory obligations to provide full and frank information on a regulatory reference.

At what point do you notify the regulator of the alleged breach?
At the very outset, the FCA and/or PRA may need to be notified if you launch an internal investigation into misconduct on the part of a Senior Manager (using Form D). If you decide to suspend a Senior Manager, the relevant regulator will need to be notified that a qualified Form C (which is required when an individual ceases to perform a controlled function) will be submitted. Equally, if an individual resigns whilst under investigation by the firm, the regulator will need to be notified, as soon as practicable, that a qualified Form C will be submitted.

If the firm takes disciplinary action against the employee and the reason amounts to a breach of a Conduct Rule, the PRA and/or FCA will need to be notified. Disciplinary action includes the issuing of a formal written warning, a suspension, as a disciplinary sanction, or dismissal of that person or the reduction or recovery of any of such person's remuneration. If an employee has misused confidential or proprietary information relating to the firm, its clients or intermediaries, this may constitute a breach of Conduct Rule 1 (to act with integrity) or Conduct Rule 2 (to act with due skill, care and diligence). Therefore, if disciplinary action is taken, a notification will be required. For FCA Certification Staff the notification is made annually, while for Senior Managers and PRA Certification Staff the notification must be made within seven business days.

It should be noted that separate notification obligations may arise if the conduct amounts to a "significant breach of a rule", by the firm or the individual, and the firm should also have regard throughout to its obligations to provide the regulators with information that the regulators would reasonably expect notice of.

Summing up
SMCR adds an extra layer of regulatory and employment law considerations when Senior Managers and Certification Staff are the subject of disciplinaries.

FIVE KEY POINTS TO REMEMBER:

1. Avoid an automatic decision to suspend, and quickly establish reasonable grounds.
2. Ensure you have temporary cover in place, with the necessary pre-approval/ certification if required.
3. Encourage the drafting of a living handover.
4. Ensure you do not compromise your regulatory obligations to provide full and frank information on a regulatory reference.
5. Ensure there is a clear understanding as to the timing of any notifications to the PRA and/or FCA.

BANKING REFORM

HAS THE FCA GONE SOFT?

The FCA is supplementing its ‘hard’ supervisory and enforcement powers with an increasing interest in softer subjects, such as behavioural economics. Polly James and Adam Turner explore the FCA’s latest theory on how to improve the culture within banking (clue – it doesn’t involve fines).

STEPS TO IMPROVE PERFORMANCE MANAGEMENT

- Moderate appraisal forms across your organisation to ensure consistency
- Review your appraisal system to ensure all KPIs are documented adequately
- Train managers to emphasise non-financial KPIs in appraisals
- Ensure consequences of missing behavioural KPIs are comparable to missing financial targets
- Use a mix of qualitative and quantitative KPIs

These days we are used to hearing the FCA making speeches about bringing more criminal prosecutions, strengthening individual accountability, and increasing the number of enforcement investigations it takes on. So it seemed a little odd to hear the FCA's Head of Retail Supervision, Jonathan Davidson, use a recent platform to discuss the collection of children from day nurseries.

Why was Jonathan Davidson suddenly talking about babies? He was using a real-life example to talk about human psychology – continuing a trend that we have been seeing increase in momentum in recent years, towards the FCA recognising the power of insights from behavioural economics in furthering its statutory objectives.

For example, in its recent work on general insurance renewals, the FCA used insights from behavioural psychology to inform the new rules it put in place for insurance renewal notices (see FCA Occasional Paper no. 12: "Encouraging Consumers to Act at Renewal").

Are fines an effective deterrent to bad behaviour?

Mr Davidson's speech outlined the results of an experiment performed by behavioural economists on parents using day nurseries. The economists introduced a system of fines to punish parents who collected their children late. The result was that more parents collected their children late. Why? Because "nurseries had reduced the decision to a commercial one and had defined the cost of tardiness… parents were prepared to pay for the convenience of being able to arrive half an hour late".

Mr Davidson concluded that "an ethical culture can be more powerful than one based solely on financial incentives." You change behaviours, Mr Davidson is saying, not by fining people who misbehave, but by insisting upon the importance of ethical behaviours.

The four levers to change corporate culture

The consequences of this policy statement are quite profound for the FCA as conduct regulator, and in particular for the FCA's interest in changing banking culture. In the same speech, Mr Davidson spoke about four levers that can be used to change the culture in a bank. Some of these levers echo familiar themes, such as setting a sound tone from the top and building solid governance structures. But the fourth of the FCA's levers is a less well-developed theme: people-related practices, including incentives and capabilities.

This speech helps to explain why the FCA has recently been so focused upon assessing firms' performance management systems. By performance management the FCA means not only the processes that are used by firms for managing under-performers, but anything that drives how people behave at work – including day-to-day interactions with their managers, incentive structures and formal performance assessment processes, such as annual appraisals. There has been a proliferation of remuneration codes in recent years – policing how much people working in financial services can get paid – but the FCA is starting to ask whether we shouldn't instead be looking at what people are being paid to do .

Encouraging desirable behaviours

The Parliamentary Commission on Banking Standards found that people were being paid too much for doing the wrong things – to date the FCA has been mostly focused on the amount of remuneration, without also considering the practical ways in which people were being persuaded towards doing wrong (or right) things. That is now changing.

Andrew Bailey, FCA CEO, recently said: "A question we seek to answer is whether practices such as recruitment, performance management, reward and capability drive positive behaviours and create a culture that works in the long term interests of a firm, its customers and market integrity". He went on to state that "It is for firms to… identify the drivers of behaviour within the firm and control the risks that these drivers create".

We predict that, given the FCA's growing interest in this area, firms will increasingly be asked to describe and justify their capability and performance management procedures, and to demonstrate how they satisfy themselves that these procedures are generating desirable behaviours and customer outcomes.

What can you do to be ready?

1. **Review the Key Performance Indicators** (KPIs) used throughout your business to assess performance. Is there an appropriate mix of qualitative and quantitative KPIs?
2. **Review the procedures used for assessing individuals** against their KPIs. Are the consequences of missing a KPI comparable across e.g. financial and behavioural KPIs?
3. **Train those managers who conduct appraisals.** Do they know that if they spend 90% of the appraisal meeting discussing financial KPIs, they are sending a clear message about the relative (low) value of the non-financial KPIs? Focus especially on your middle managers, who may be in the most difficult position because they have financial targets that they must meet, but often no direct customer contact.
4. **Take a hard look at your appraisal system.** Does it capture documentary evidence of each individual's performance against both financial and non-financial KPIs, such that you can prove when the FCA asks if you have really been assessing both aspects?
5. **Set up a process of independent moderation** of appraisal forms to ensure consistency across the business. In view of Jonathan Davidson's recent comments discussed above, under SMCR, this is especially important for the Senior Manager who has the prescribed responsibility for culture within the firm.

> A question we seek to answer is whether practices such as recruitment, performance management, reward and capability drive positive behaviours and create a culture that works in the long term interests of a firm, its customers and market integrity
>
> Andrew Bailey, FCA CEO

Polly James
Partner,
Financial Services
Investigations

Adam Turner
Associate Director,
Employment

REGULATORY CALENDAR

EXPECTED DURING

QUARTER ONE

JAN 2018

1 January – Date from which the PRIIPs Regulation and the Commission Delegated Regulation on KIDs for PRIIPs will apply in member states.

Effective date for application of the Benchmarks Regulation across the EU.

Date on which European Commission intends the proposed Regulation amending the CRR in relation to IFRS 9 to apply.

Date on which BCBS expects member states to apply leverage ratio as a Pillar 1 minimum requirement.

Date on which BCBS expects member states to apply net stable funding ratio (NSFR) as a minimum standard.

Closing date for responses to chapter 6 of FCA CP17/39 concerning the FCA's proposed amendments to the Enforcement Guide and the Supervision manual (SUP) relating to the IDD.

3 January – Amendment to the definition of financial advice for regulated firms in article 53(1) RAO will take effect.

Effective date for application of provisions in MAR to organised trading facilities (OTFs), SME growth markets, emission allowances or auctioned products based thereon (to the extent the relevant provisions refer to these items).

Date from which MiFID II and MiFIR are to apply.

Entry into force of new rules on transaction cost disclosure in workplace pensions set out in the Pension Schemes (Disclosure of Transaction Costs and Administration Charges) Instrument 2017 (FCA 2017/53).

FCA final rules come into force on standardising disclosure of transaction costs incurred by pension investments (CP16/30) in accordance with the policy set out in PS17/20.

5 January – Closing date for responses to EIOPA's November 2017 consultation paper on a second set of advice to the European Commission on specific items in the Solvency II Delegated Regulation.

8 January – Closing date for responses to the IAIS' November 2017 consultation papers on draft revisions of ICPs 8, 15 and 16, the associated ComFrame materials and proposed definitions of terms related to enterprise risk management.

13 January – Deadline for EU member states to transpose PSD2 into national law. The Payment Services Regulations 2017 (SI 2017/752), which will repeal and replace the Payment Services Regulations (SI 2009/209), enter fully into force.

Date of application of EBA guidelines on remuneration policies and procedures related to the sale and provision of retail banking products and services.

19 January – Closing date for comments on FCA's November 2017 terms of reference for its market study on competition in the wholesale insurance sector.

January – FCA expected to publish policy statement to its third consultation paper on the implementation of the IDD (CP17/33).

FEB 2018

By February – EIOPA intends to send its second and final set of technical advice to the European Commission relating to the review of the Solvency II Delegated Regulation.

1 February – Closing date for comments on chapter 4 of FCA CP17/39 concerning proposed amendments to the DISP rules relating to the requirements in MLR 2017 that provide for enhanced due diligence when firms are dealing with PEPs, their family members or known close associates.

19 February – Deadline for responses to the FCA's further consultation on retiring finalised guidance on inducements and conflicts of interest (FG14/1) and on independent and restricted advice (FG12/15).

21 February – Deadline for responses to FCA CP17/40, CP17/41 and CP 17/42 and PRA CP28/17 concerning the implementation of the extension of the senior managers and certification regime (SM&CR) to FCA solo regulated firms and insurers.

23 February – IDD transposition deadline: UK regime transposing and implementing IDD expected to come into force.

27 February – Deadline for responses to PRA Consultation Papers 29/17 and 30/17 into the Bank of England's approach to the authorisation and supervision of international banks, insurers and central counterparties.

28 February – EIOPA to submit final technical advice to European Commission regarding Commission's review of specific items in the Solvency II Delegated Regulation (Regulation (EU) 2015/35) as regards unjustified constraints to financing.

MAR 2018

1 March – New FCA rules introducing an information prompt in the annuity market, as set out in PS17/12, come into force.

By 31 March – European Commission to publish an EU strategy for FinTech, including an EU licensing and passporting framework for FinTech.

EXPECTED DURING QUARTER TWO

APR 2018

6 April – Deadline for implementation of the ABI voluntary guide to simplifying language on retirement options.

FCA Handbook rule changes in Conduct of Business Sourcebook (Pension Projections) Instrument 2017 (FCA 2017/43) come into force. This follows proposals in quarterly CP16/39 regarding the format of personalised projections and feedback in FCA Handbook Notice 46.

April – Deadline for credit card firms to comply with agreed industry standard to:

- Inform customers when their credit card promotional offer is due to end.
- Allow credit card customers to request a "later than" payment date to give greater control and help them avoid penalty charges.

MAY 2018

9 May – Date by which member states are required to have transposed the Cyber-security Directive.

10 May – Date from which national measures transposing the Cyber-security Directive apply.

JUN 2018

30 June – Date by which EIOPA is required to submit (first) final draft RTS under Article 10(7) of the IDD, relating to adapting certain amounts in euro, to the European Commission.

By June – FCA expected to complete reviews of insurance pricing practices and value in the insurance distribution chain.

By end Q2 – FCA to complete financial crime thematic review of e-money, as per the FCA's 2017/18 business plan.

FCA to publish the final report on its retirement outcomes review.

ESMA to publish a final report setting out guidelines on MiFID II suitability requirements.

FCA expected to publish a project update on its strategic review of retail banking business models.

EXPECTED DURING QUARTER THREE

JUL 2018

21 July – The MMF (Money Markets Fund) Regulation enters into force.

July – Deadline for credit card firms to comply with agreed industry standard to notify customers when they are close to their credit limits to help avoid penalty charges.

AUG 2018

August – FCA expected to publish interim report on how firms are handling complaints about payment protection insurance (PPI).

By end Summer – FCA and PRA expected to publish policy statements and final rules relating to the extension of the SMCR to all FSMA authorised firms.

SEP 2018

By 1 September – HM Treasury review of the Mortgage Credit Directive ((EU) 2014/17) (MCD) implementation.

1 September – Deadline for relevant firms to comply with the MiFID II systematic internaliser (SI) regime.

30 September – Date on which FCA Handbook rule changes set out in the Retirement Income Data (Regulatory Return) Instrument 2017 (FCA 2017/48) come into force, in accordance with FCA policy set out in PS17/16 (Regulatory reporting: Retirement income data Feedback on CP16/36 and final rules).

EXPECTED DURING
QUARTER FOUR

OCT 2018

By October – Financial Action Task Force (FATF) expected to carry out its fourth mutual evaluation of the UK.

NOV 2018

By 1 November – Association of British Insurers (ABI) to make recommendation as to whether code of good practice, designed to help insurers and insurance brokers provide support to potentially vulnerable customers when renewing motor and household insurance policies, should continue in its current or an amended form.

9 November – Date by which each member state is required to identify the operators of essential services within an establishment on their territory under the Cyber-security Directive.

DEC 2018

By December – European Commission intends to have completed its review of specific items relating to the standard formula under the Solvency II Delegated Regulation.

European Commission expected to finish assessment of priority 1 third countries under Article 9 of MLD4, using new assessment methodology.

European Commission expected to adopt Delegated Regulation under Article 9 of MLD4, using new assessment methodology.

SMCR to be extended to insurers (subject to the commencement date set by HM Treasury).

FCA expected to complete thematic review of fair treatment of with-profits customers.

31 December – Deadline by which the European Commission must review the PRIIPs Regulation.

By end Q4 – European Commission expected to carry out an assessment of whether Solvency II should be amended in relation to the prudential treatment of private equity and privately placed debt.

STRATEGICALLY NAVIGATING THE THREAT OF ENFORCEMENT

How the BLP Financial Regulation team helped one firm challenge the FCA to avoid enforcement

Under pressure

A firm has received notification that it is subject to an enforcement investigation and needs legal representation.

Risk & Compliance Director phones BLP

We review the relevant documents in detail and find a defence angle that our competitors have overlooked.

A refreshingly determined approach

BLP is instructed due to our "refreshing attitude", willingness to "robustly defend" and "having insight into how the FCA operates".

Sound strategic thinking

The BLP team identify key areas to challenge the FCA's decisions and devise a clear strategy ahead of meeting the firm.

Fast and effective execution

Our defence strategy involves taking proactive steps to convince the regulator that its case is legally flawed. We execute the strategy with energy and determination, securing an early notice of discontinuance.

> "For me, they represented someone who was prepared to fight for us"

About BLP

Berwin Leighton Paisner is an award-winning, international law firm. Our clients include over 50 Global Fortune 500 or FTSE 100 companies. Our global footprint of 13 international offices has delivered more than 650 major cross-border projects in recent years, involving up to 48 separate jurisdictions in a single case.

The Firm has won eight Law Firm of the Year titles, is independently ranked by Chambers and the Legal 500 in over 65 legal disciplines and also ranked in 'the top 10 game changers of the past 10 years' by the FT Innovative Lawyers report 2015.

Expertise

- Antitrust & Competition
- Commercial
- Construction
- Corporate Finance
- Dispute Resolution
- Employment, Pensions and Incentives
- Energy and Natural Resources
- Finance
- Insurance
- Intellectual Property
- Investment Management
- Private Client
- Projects and Infrastructure
- Real Estate
- Regulatory and Compliance
- Restructuring and Insolvency
- Tax

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

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

Clients and work in 130 countries, delivered via offices in:
Abu Dhabi, Beijing, Berlin, Brussels, Dubai, Frankfurt, Hong Kong, London, Manchester, Moscow, Paris, Singapore, Tel Aviv and Yangon.

www.blplaw.com