BCL Solicitors LLP

LondonCalling

March 2017

Introduction

Welcome to our latest update on corporate crime, investigations and regulation. In this edition, we look at the UK prosecuting authorities' increasingly assertive approach with fresh developments in the struggle over legal privilege and forthcoming AML powers. We also examine why, as the UK heads towards exiting the EU, corporates must continue to keep an eye on their potential exposure to criminal prosecution in respect of data protection, data transfer and surveillance measures influenced by Europe.

Has Legal Advice Privilege been eroded in corporate investigations?

Harry Travers and Alex Swan consider the impact of the High Court's decision in Re RBS Rights Issue Litigation [2016] EWHC 3161 (Ch).

As reported in our September 2016 edition of LondonCalling, battle lines between investigatory authorities, principally the SFO, and corporates have for some time been drawn over the issue of legal professional privilege (LPP). The SFO has threatened to challenge "false and exaggerated claims" while professional guidance for lawyers has re-stated the importance of LPP in forthright terms. A recent High Court decision on the scope of LPP in the civil dispute between Royal Bank of Scotland (RBS) and shareholders has highlighted some of the issues in the ongoing debate.

A real distinction "...between reflecting 'a train of inquiry' and reflecting or giving a clue as to the trend of legal advice."

Dealing first with the claim to legal advice privilege, RBS submitted that the communication of factual information (i.e. notes) gathered by or for the purpose of being provided to its lawyers, where the submitting party was authorised to do so by RBS, was privileged as it was done so for the purpose of enabling RBS to seek legal advice. However, the claimants argued that the communication of factual information by a company employee to the company's lawyers was not privileged, and legal advice privilege covered only communications between a client and his lawyer for the purpose of the lawyer giving, and that client seeking or receiving, legal advice.

The High Court was bound to follow a previous (often criticised) decision of the Court of Appeal in *Three Rivers (No 5)*, in which it ruled that in a corporate context information gathered from an employee is no different to information obtained from third parties, even where the information was obtained in order to be shown to a lawyer to enable fully informed advice to be given to the lawyer's client. RBS sought to distinguish *Three Rivers* on the basis that direct communication by an authorised employee to the corporate's legal adviser in a corporate context had not been addressed in that case.

Despite recognising the cogency of RBS' submissions, the judge rejected RBS' argument, finding that *"the individuals interviewed were providers of information as employees and not clients...and* [the notes] *were not communications between client and legal adviser."*

RBS alternatively sought to argue that the notes were privileged on the basis that they constituted lawyers' working papers, as the non-verbatim notes had been prepared by lawyers, reviewed by lawyers as being subject to privilege, contained notes recording that they reflected lawyers' *"mental impressions"*, and revealed the lawyers' train of inquiry. Again, though, the judge ruled against RBS, and found that the evidence did not support RBS' contentions – the evidence had to be more than "*conclusory in nature*" – the judge remarked that it was rather telling what the evidence did not show, and found that there was a real distinction *"...between reflecting 'a train of inquiry' and reflecting or giving a clue as to the trend of legal advice."*

Finally, in dealing with RBS' arguments that under US law the notes would have been privileged, the judge was prepared to assume that was so but held that there was no sound basis for disturbing the usual practice of applying the law of forum, i.e. English law.

It is of note that the judge was not unsympathetic to some of RBS' arguments. The *Three Rivers* decision has often been criticised, and, given the current preponderance of multi-jurisdictional corporate investigations, it was initially hoped that the time may have arrived for this decision to be reviewed. However, RBS have now confirmed that they will not be appealing this judgment as the claimants are no longer seeking the documents which were the subject of the High Court decision.

Litigation privilege was not invoked but rather legal advice privilege...

This means that, for now, the *Three Rivers* decision will stand and corporates will continue to face a difficult task when deciding whether the products of their investigations are covered by legal advice privilege. In circumstances where many cases can now involve simultaneous cross-border investigations, more care than ever needs to be taken in determining the different approaches to privilege in different jurisdictions and developing an appropriate global strategy accordingly.

Additionally, corporates and lawyers will need to give careful thought to who the "client" is in order safely to claim privilege. In asserting such a claim, clear and cogent evidence as to the type of legal input involved will need to be provided, rather than simple 'conclusory' assertions.

It should be noted that in *Re RBS Rights Litigation*, litigation privilege was not invoked but rather legal advice privilege (which can be wider) was claimed. It may be that a claim to litigation privilege, where litigation is clearly in contemplation, has a better chance of success, but in corporate investigations it may not always be possible to demonstrate, especially at an early stage of the internal investigation, that the dominant purpose of a communication or document was for litigation.

Harry Travers *is a partner specialising in corporate crime and regulation. He has vast experience in high-profile white collar crime/regulatory investigations conducted by the leading government agencies, often with a wide-ranging international dimension. Top-ranked in both Chambers UK and Legal 500, he is one of only two lawyers specialising in business corporate crime listed in the Chambers 100.*

Alex Swan *is a solicitor specialising in corporate crime. He has considerable experience of dealing with corruption, money laundering, and fraud matters, including cross-jurisdictional investigations.*

Electronic Surveillance: a (not so) brave new world?

Michael Drury and Luke Clements consider the public response to the Investigatory Powers Act 2016 and the ensuing debate surrounding internet connection records.

The Investigatory Powers Act 2016 receives Royal Assent
The Investigatory Powers Act 2016 (IPA) – known colloquially as the "Snooper's Charter" – has been one of the most hotly debated laws of recent times. The product of Theresa May's tenure as the Home Secretary, NGOs and opponents now suggest there was insufficient scrutiny given by Parliament during its passage.

The IPA received Royal Assent on 29 November 2016 and has now become law

Weighing in at almost 300 pages and comprising of 272 sections, ten Schedules and six detailed draft Codes of Practice, it is by no means a simple piece of legislation. However, after almost a year of debate, and a swift passage through its final Parliamentary stages, the IPA received Royal Assent on 29 November 2016 and has now become law. But, what does it do – and aside from the effect of court challenges to the existing law (see our separate commentary on *Watson*) – what are the issues now arising?

Background
The IPA was introduced in response to heightened criticism of the surveillance activities undertaken by public authorities in the UK. This was at a time when the Snowden revelations, and the litigation that ensued, had led to an outcry by NGOs and interest groups as to the Government's collection and use of communications and communication data.

When drafting the IPA, the Government sought to codify the existing laws governing data monitoring into one single legislative scheme. The aim of doing so was to ensure that public authorities, particularly law enforcement agencies and the security and intelligence services, had powers that were not only fit for the digital age but also human rights compliant.

The public response
Notwithstanding the (eventual) Parliamentary consensus, what has been remarkable is the negative public reaction to the IPA passing into law. This is most apparent in relation to the introduction of powers relating to internet connection records (ICRs), which have been the topic of much of the dissatisfaction surrounding the IPA.

To illustrate the public discontent, a petition to repeal the IPA, posted on Parliament's website, has garnered over 206,000 signatures; this is unprecedented in respect of new legislation. Unsurprisingly the Parliamentary Petitions Committee decided not to hold a debate on this petition, citing the fact that the IPA had previously been debated on many occasions and had already been the subject of scrutiny by an expert committee. Nevertheless, the sheer number of signatories to the petition reflects a potential post-Brexit shift in social attitudes, whereby the public are now more willing (and eager) to come together to challenge the legitimacy of decisions made under the aegis of democracy, particularly when a decision has the potential to impact on their human rights or freedoms. In a further display of discord, human rights campaign group, Liberty, has started a crowdfunding appeal to underwrite a judicial review of the IPA. The appeal has quickly reached its initial target (over £50,000 in donations) and continues to gain momentum. In a time of austerity, this level of support is striking and should not go unnoticed.

Internet connection records – not all they are cracked up to be?
Powers relating to ICRs are one of the most – if not the most – contentious aspects of the IPA. For many, the retention and disclosure of ICRs are seen as excessively intrusive and out of sync with human rights obligations.

Broadly speaking, an ICR is capable of constituting a range of data showing: **when** a connection was made; **where** a device was located when making the connection; **what** service a device accessed; and **who** made the connection i.e. what device was used. However, as a matter of law an ICR will not show what an individual did on a particular website. This means that public authorities that acquire ICRs will be able to see that a device accessed a given website on a specified day, but an ICR will not show the images, content, communications etc. that were accessed using that website.

This does little to dissuade some critics, who argue that the collation and retention of such data is still grossly invasive and open to exploitation. In some respects this opposition is justified; the websites we visit have the potential to disclose deeply personal information about us. Whether it relates to health, addiction, infidelity or sexual preferences – to name a few – there are many who would rather keep such information private and out of the hands of the Government (or, worse yet, the hands of hackers).

For many, the retention and disclosure of ICRs are seen as excessively intrusive and out of sync with human rights obligations

The limited nature of ICRs also presents an issue for public authorities – particularly law enforcement – who will undoubtedly be left to question their usefulness as an essential investigative tool. It will be an uphill struggle to build an accurate picture of an individual's online activities without knowing what the individual did on a given website. This is most prominent where ICRs are obtained for the prevention and detection of criminal activity. In this case, it is of limited use to know that an individual visited a particular website (albeit potentially one that is unlawful in its content). Instead a public authority will want to know what the individual did on the website, what images were uploaded or downloaded, or what posts were made.

It is only a matter of time before the Home Secretary uses her discretionary powers to bring the remaining sections into force

Conclusion

The enactment of the IPA has already commenced, with the data retention provisions having come into effect on 30 December 2016. We assume it is only a matter of time before the Home Secretary uses her discretionary powers to bring the remaining sections into force, although there seems to be no obvious urgency. However, given the breadth of criticism of the IPA, one is left to wonder whether the Government would be so attached to the Act had the current Prime Minister herself not invested so much personal capital in its success.

Michael Drury *is an expert in surveillance, cybersecurity law and cybercrime. Before joining BCL he was Director of Legal Affairs at GCHQ (the UK equivalent of the NSA) responsible not only for legal advice on the UK Government obtaining data in the interests of its national security, but also in the protection of data by the UK Government. He combines that experience in maintaining his present practice in that field with defending clients in high profile and corporate crime cases.*

Luke Clements *is a solicitor specialising in all aspects of corporate crime. Having previously worked for the SFO, he has considerable experience across a broad range of bribery and fraud investigations, including the exercise of powers of compulsion.*

Back to the drawing board thanks to the CJEU's judgment in Watson & Ors

Michael Drury and Julian Hayes explain why already repealed data retention legislation is still causing the UK Government a headache.

On 21 December 2016, the European Court of Justice (CJEU) handed down its long awaited decision in a high-profile privacy challenge brought by MP Tom Watson and others. The judgment took the shine off the Government's newly enacted Investigatory Powers Act (IPA).

The challenge had been brought against the Data Retention Investigatory Powers Act 2014 (DRIPA) which empowered the Secretary of State to require telecoms operators to retain relevant telecommunications data (for example, data necessary to identify the source, destination, time, date, duration and type of a communication) for reasons such as national security, the prevention or detection of crime and the prevention of disorder.

Given that DRIPA contained a "sunset clause" causing it to expire on 31 December 2016 anyway, the proximity of the CJEU judgment to the Act's expiry might have consigned *Watson & Ors* to relative legal obscurity, had not DRIPA's provisions been substantially incorporated into the IPA, the data retention sections of which were brought into force on 30 December 2016. As a result, the judgment has become highly significant to the Government, to law enforcement capability (and by extension the general public) and to telecoms operators receiving IPA retention notices in future.

The CJEU Judgment

In giving judgment, the CJEU explained the significance of the data concerned. It allowed very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained – their everyday habits, places of residence, daily movements, activities and social relationships. Taken as a whole, the DRIPA retention requirements represented a particularly serious and far-reaching interference with the EU Charter rights to respect for private and family life and for the protection of personal data.

The judgment has become highly significant to the Government

Interference with such fundamental rights must be clear and precise in scope and application and must be strictly necessary and proportionate to the end sought, be that safeguarding national security, defence and public security or the prevention, detection and prosecution of crime. Where the aim is the fight against crime, only serious crime justifies the interference with EU Charter rights. Most significantly, the fight against serious crime, in particular organised crime and terrorism, could not alone justify national legislation providing for "*the general and indiscriminate retention of all traffic and locations data*".

Whilst the general retention of data infringes EU Charter rights, national laws could permit the *targeted* retention of data if, based on objective evidence, it were first possible to identify a section of the public whose data is likely to reveal at least an indirect link with serious criminal offences or prevent a serious risk to public security.

Targeted retention might be justifiable where there is a high risk that individuals in a particular geographical area might be involved in preparing to commit a serious crime. The Court did not give guidance on the potential size of such geographical areas, nor did it expressly exclude the possibility that other limits besides geography might be applied if objective data justifies it. This unhelpfully opens up the damaging possibility that a member state could seek in future to retain data on the basis of ethnicity or religion, causing potential friction with equalities legislation, although doubtless the CJEU will require something more precise to justify selection on objective evidence.

Only the objective of fighting serious crime is capable of justifying such access to the retained data

Where targeted data is retained, access to it must correspond to the criterion for its retention – where crime fighting is concerned, "*only the objective of fighting serious crime is capable of justifying such access to the retained data*". Generally, access can only be granted to the data of individuals suspected of either planning to commit, having committed, or being implicated in connection with a serious crime. However, in an ambiguous passage highlighting the tension which many people feel between the competing priorities of privacy and combating crime (particularly after recent violent atrocities in Europe), the CJEU stated that access to the data of individuals who are not suspects might also be granted where it could be shown that it would make an "effective contribution" in combating specific terrorist threats to vital national security, defence or public security interests.

National legislation must make provision for retained data to be held within the EU

Perhaps the clearest and most crucial element of the judgment is that access to retained data must be proportionate and must normally be authorised by a Court or independent administrative body. Data subjects must be notified if their data has been accessed once doing so would no longer jeopardise an ongoing investigation. Finally, in a move with potential practical implications for telecoms operators served with retention notices, national legislation must make provision for retained data to be held within the EU. This latter point is a new and potentially significant development.

Access to retained data must be proportionate and must normally be authorised by a Court or independent administrative body

Impact on the IPA
Watson & Ors places the CJEU on an immediate collision course with the IPA. At present, Part 4 of the IPA permits the retention of data for a whole raft of reasons besides national security and crime fighting, including the protection of public health, assisting in investigations of miscarriages of justice, assisting in identification of someone who has died or who is too ill to identify themselves, for the regulation of financial markets and for the collection of taxes.

As a result of the CJEU decision, none of these reasons will legally justify data retention even though many people may regard them as justifiable.

Similarly, retention notices requiring the retention of "all data or any description of data" may now be too broad without qualification by reference to a geographical limit based on a particular threat.

Non-universal data retention will inevitably be less effective as a crime fighting measure (or as a means of preventing atrocities that are in themselves seen as crimes as well as threats to national security)

However, as the UK's Independent Reviewer of Terrorist Legislation has indicated, because suspects are often not known in advance, the more limited data retention now permitted may well miss the perpetrators of offences who had not previously come to the attention of the authorities and who could not, therefore, be targeted in advance. In other words, non-universal data retention will inevitably be less effective as a crime fighting measure (or as a means of preventing atrocities that are in themselves seen as crimes as well as threats to national security). It is a matter of ongoing moral debate whether the collateral intrusion on the data of innocent people inherent in the generalised data retention, as advocated by the UK Government, is a price worth paying in the fight against crime.

When Part 3 of the IPA comes into force, a designated senior officer from one of 48 public authorities will have the power to grant access to retained data for the purpose of a specific investigation or operation for a number of statutory reasons. Such powers are likely to be challenged by privacy campaigners at an early opportunity. Real questions arise about the compatibility of the IPA and the existing RIPA requests that still remain in force.

Finally, the requirement to notify data subjects that their personal data has been accessed once an operation is over risks placing a costly administrative burden on the authorities responsible, potentially undermines the effectiveness of future security operations and may overwhelm and alarm those receiving such notification.

It is likely that the Government will have to amend the IPA

Outlook
The matter now returns to the UK's Court of Appeal for a decision on the operation of DRIPA (and by implication the IPA's data retention provisions). In due course, it is likely that the Government will have to amend the IPA. In the meantime, those tempted to look to Brexit as a solution to the legislative dilemma may be disappointed; if Britain wishes to maintain the free flow of data with member states after its eventual departure from the EU, it will be obliged to provide "essentially equivalent" data protection to that provided within the EU; a refusal to amend the IPA in conformity with this and future CJEU judgments may well curtail such data flows with significant consequences for the UK's economy.

Michael Drury CMG, *Partner*

Julian Hayes *is a partner specialising in all aspects of corporate crime and regulatory work. As well as dealing with high profile fraud and corruption matters, including investigations with an international dimension, he has considerable experience of advising corporates on data protection and cybercrime issues.*

The UK Anti-Money Laundering Regime: the practical effects for business

John Binns and Caroline Mair discuss the key provisions of the UK Anti-Money Laundering regime, a regime which has serious and wide-ranging implications for business. The authors provide a snapshot of those provisions and some practical guidance on how businesses might wish to approach their anti-money laundering responsibilities.

The UK's money laundering legislation is complicated and far-reaching. Although its main impact is on the banks and others in the "regulated sector" of the UK itself, it has the potential to impact on any business in any sector, anywhere in the world. It is important therefore for businesses to be aware at least in broad terms of the legislative landscape and the pitfalls that may arise.

Key Provisions

The main statutes of which businesses need to be aware are the Financial Services and Markets Act 2000 (FSMA) and the Proceeds of Crime Act 2002 (POCA). Although it is POCA that defines the principal money laundering offences (as well as, for example, setting out regimes for confiscation and civil recovery of criminal assets), it is under FSMA that the Money Laundering Regulations 2007 (MLR) are made, which define the obligations of those in the "regulated sector" – originally comprising banks and financial institutions, but now including many others including accountants and (in some cases) solicitors.

The principal money laundering offences in sections 327 to 329 of POCA are very broadly worded and in essence prohibit doing anything with assets, including merely possessing them, where such assets are or represent the "proceeds of crime".

Assets include money and "pecuniary advantages". It should be noted that the offences are committed where the person dealing with the assets either knows or even merely suspects their criminal origin (which makes them "criminal property" for the purposes of POCA). Under a recent controversial Court of Appeal case, the UK courts decided they have universal jurisdiction to try any allegation of money laundering wherever and by whomever it is said to have been committed.

Later sections of POCA create offences specific to the regulated sector, which is also subject to requirements under MLR, for instance to perform "Anti Money Laundering" (AML), Customer Due Diligence (CDD) and "Know Your Customer" (KYC) procedures, especially where there are considered to be heightened risks including the involvement of "Politically Exposed Persons" (PEPs). The effect of this is that banks, accountants and others are obliged to research their customers and submit a suspicious activity report (SAR) to the National Crime Agency (NCA) where there is a "reasonable cause" for suspicion, or face criminal sanctions in default. Importantly, POCA also criminalises "tipping off" the subject of a SAR and prejudicing any investigation into them.

Potential Defences to Money Laundering Offences

There are also defences available in relation to all of the offences where the person submits a report to the authorities as soon as reasonably practicable and, if the report precedes the act in relation to the asset, he obtains consent for it. POCA's "consent regime" sets out a timetable by which, when a SAR is submitted, the NCA has an "initial notice period" of seven working days to refuse consent, followed by a "moratorium period" of 31 calendar days after which (absent action by the authorities to freeze the assets) consent can be assumed. The NCA has been careful to point out however that submitting a SAR should not be used as a substitute for taking a risk-based approach in assessing the money laundering risks facing a business; perhaps this says something about the workload of the NCA given the implication that those submitting a SAR are not making well-balanced decisions.

What are the implications of the Money Laundering regime for businesses?

The implications of this regime for a business that, for instance, discovers a risk that an employee or agent has committed a bribery or fraud offence, are potentially both complex and serious. If, say, a bribe has been paid to obtain an advantage for the business, or if its accounts have been used as a conduit for a fraud, then the business may in effect be "in possession" of criminal property if and from the moment that it suspects that this is the case. Depending on the answers to these questions, it may be necessary, prudent or even advantageous to submit a SAR to the NCA, and seek consent to deal with the assets.

Meanwhile, any business that deals with banks or others in the UK's regulated sector should also be aware of the risk that, quite apart from the above, a SAR might be submitted in respect of their own assets, most typically in respect of their bank accounts. Increasingly, the UK's banks, being understandably risk-averse in this sector, will decide to close or block accounts at the slightest hint of any matter that could give rise to a "reasonable cause for suspicion" – which they would doubtless consider a very low threshold – and because of the provisions on "tipping off", adopt a firm policy of refusing to discuss these matters with their customers. Often the first indication that a business will have of being the subject of any such attention is an unexplained block on its accounts, or a failure by the bank to carry out a transaction.

UK banks will decide to close or block accounts at the slightest hint of any matter that could give rise to a "reasonable cause for suspicion"

In both scenarios, it will often be prudent for a business against whom a SAR has been submitted to take proactive steps to contact (directly and/or via the bank or other reporter) the NCA and any investigators, offering cooperation, while meanwhile conducting its own enquiries into the likely cause of the difficulty.

An effective set of representations within the "initial notice period", including explanation of the business rationale of particular transactions potentially giving rise to suspicion, may cut matters short and mitigate the potential damage to the business: failing that, the accounts may be blocked for the remainder of the "moratorium period" or even longer.

The future of the UK Anti-Money Laundering regime

Forthcoming changes to the legislation will make matters more difficult for businesses, including a facility for the authorities to extend the "moratorium period" a further six times, and measures under the latest (Fourth) EU AML Directive to tighten up AML procedures, including for example a broader definition of PEPs. Legislators, of course, would argue that these measures are necessary to protect the public from the effects of acquisitive crime. Though few would argue against that aim, the practical impact is a set of potential criminal liabilities of which *all* businesses need to be aware and against which they must seek to protect themselves.

John Binns *is a partner with particular expertise in confiscation, money laundering and civil recovery proceedings under the Proceeds of Crime Act 2002, as well as the anti-money laundering and sanctions compliance procedures of the UK regulated sector.*

Caroline Mair *is an employed barrister specialising in corporate crime and regulatory enforcement, with a particular focus on criminal fraud. She has been in involved in a number of high profile cases most notably in relation to an ongoing cross border investigation in relation to the alleged manipulation of LIBOR.*

In brief

A potentially significant judgment, *ERY v Associated Newspapers Limited*, was handed down by the English High Court on 4 November 2016, upholding the claimant's right to privacy and preventing the publication of the fact that the claimant was subject to a police investigation concerning allegations of financial crime.

During the course of a criminal investigation, the claimant was invited to attend an interview under caution, on a voluntary basis, following a search of the claimant's company premises. The claimant was not arrested and received an assurance that his involvement in the investigation would remain confidential.

The fact of the claimant's involvement was leaked and the Mail on Sunday advised the claimant of their intention to publish certain personal details. The claimant sought injunctive relief. In a short *ex tempore* judgment, the judge was satisfied that an injunction, prohibiting publication of the claimant's personal involvement in the criminal investigation, should be granted. At the return date, the injunction was upheld, independent of factors personal to the claimant (such as health and children), and notwithstanding the fact that the police's investigation into the claimant's company was a matter of public record.

In light of numerous examples of the press reporting the identity of individuals subject to pre-charge police investigation, this is a welcome development in the contentious debate regarding anonymity. College of Policing guidance on media relationships and the Leveson report agree that, save in exceptional and clearly identified circumstances, the names and identifying details of those **arrested** or **suspected** of a crime should not be released to the press or public.

Whilst each matter must be considered on its merits, this judgment is a positive and potentially wide-reaching decision in relation to protecting the rights of individuals under criminal investigation.

On 1 December 2016 the Competition and Markets Authority (CMA) secured its first disqualification of a director of a company for a breach of competition law.

The CMA has the power, under the Company Directors Disqualification Act 1986 as amended by the Enterprise Act 2002 (in force since 20 June 2003), to apply to the court for a disqualification order where an individual director has been found to be in breach of competition law.

In August 2016, the CMA found that the company, an online poster supplier, colluded with a competitor not to undercut their respective prices and imposed a fine of £163,371. The former managing director of the company was found to have personally contributed to the breach and was disqualified from holding company directorships, or performing certain roles, for a period of five years.

It is worth noting that this disqualification period was achieved via a "disqualification undertaking", voluntarily entered into by the former director. Bearing in mind the maximum disqualification period the CMA can apply for is 15 years, such an undertaking was presumably offered to avoid a more severe term, as well as liability for costs should the CMA have gone to court.

The other company involved in the breach of competition law reported it to the CMA and was subsequently granted immunity under the CMA leniency procedure.

This development indicates that the CMA is willing to impose significant personal sanctions upon individuals who are found to have contributed to breaches of competition law, even if those individuals are not subject to criminal process under the Enterprise Act 2002.

Gavin Costelloe *is a solicitor specialising in all aspects of serious and complex corporate criminal litigation and has acted in numerous investigations by the SFO, HMRC, CPS and CMA.*

BCL is a market leader in the UK in the areas of domestic and trans-national business crime and regulatory enforcement, providing discreet, effective and expert advice to commercial organisations, directors, senior personnel and high profile/high net worth individuals. Our reputation has been established over many years through our unremitting drive to help our clients by providing a supportive service and guidance through the legal minefield, while focussing at all times on achieving a pragmatic solution rather than burdening them with dense legal problems and process.

Our expertise covers all areas of criminal/regulatory law including commercial and tax fraud, corruption, sanctions offences, cartel activity, financial regulation and money laundering, extradition and mutual legal assistance, corporate manslaughter, health and safety, fire safety, product safety and environmental law. We also advise in the areas of anti-money laundering and anti-corruption compliance.

"BCL's attorneys seem to pop up wherever the SFO shifts its gaze." So said *Global Investigations Review* when including BCL *("a small firm with a big reputation in the area of corporate crime")* in its top 100, an annual guide to the world's leading cross-border investigations practices able to handle sophisticated cross-border government-led and internal investigations. Additionally, a number of our partners are recognised in *Who's Who Legal: Business Crime Defence; Who's Who Legal: Investigations and Who's Who Legal: 100*.

BCL has been consistently ranked as a leading firm by Chambers in its guide to the UK legal profession, achieving top-ranked status in five categories, and being ranked as a leading firm in three others. In its 2017 edition BCL was described as *"Superb – THE boutique criminal corporate and Proceeds of Crime Act outfit to go to... A premier outfit with an excellent reputation for its representation of individuals including company directors, officers and employees..."* with *"...a reputation for legal excellence which is richly deserved"* and seven of our partners were ranked in the category of *Financial Crime: Individuals*, more than any other firm. BCL is also recognised as a leading firm in the 2016 inaugural edition of Chambers High Net Worth guide.

For more information on any of the topics covered, or more generally about BCL, please contact:

Richard Sallybanks
rsallybanks@bcl.com

Brian Spiro
bspiro@bcl.com

Harry Travers
htravers@bcl.com

Michael Drury
mdrury@bcl.com

BCL Solicitors LLP

51 Lincoln's Inn Fields
London WC2A 3LZ

Telephone +44 (0)20 7430 2277
Fax +44 (0)20 7430 1101

www.bcl.com