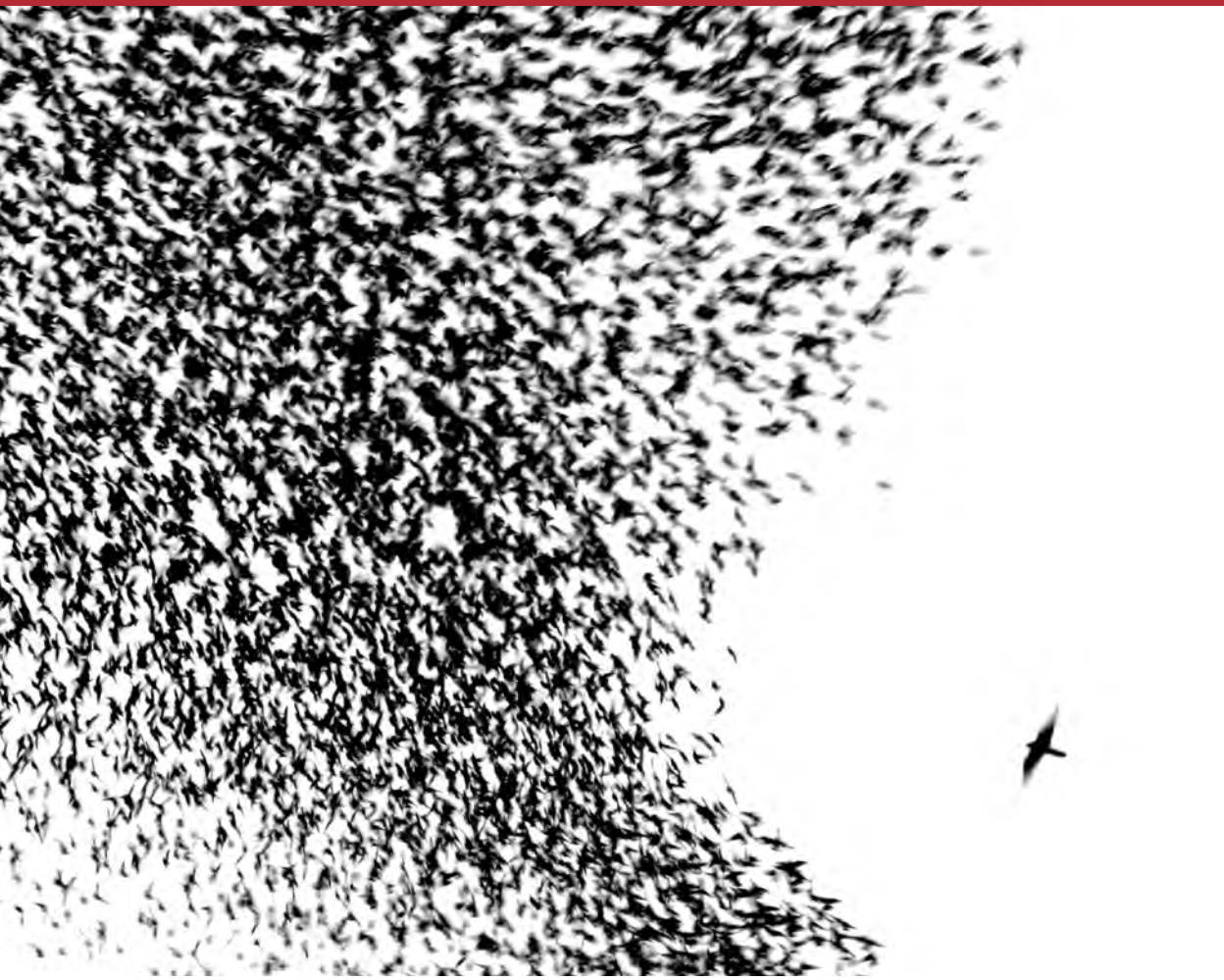
Published by White Page Ltd in association with the Serious Fraud Office

SFO serious fraud office

Serious Economic Crime

A boardroom guide to prevention and compliance



With contributions from leading advisers and featuring introductions from:

OLAF · Transparency International UK · City of London Police · Society of Corporate Compliance and Ethics · OECD · The World Bank

22

Preparing for a 'dawn raid' – and dealing with the aftermath

Peter Crowther, Partner
Winston & Strawn LLP

They happen without warning and are timed for maximum surprise. Launched by national and international authorities from the Serious Fraud Office (SFO) to the European Commission (EC), 'dawn raids' of corporate premises form the first front of investigations into suspected unlawful activities by companies and individuals. Searches for information are carried out and the aim is that, caught off guard, the target will not have the chance to hide or destroy evidence.

But while, by their nature, the raids cannot be foreseen, companies can still prepare for them by putting procedures in place, knowing their rights and understanding how to deal with the impact, both in the short and longer term, of a dawn raid.

Responding to a dawn raid

Prior to a raid

Apart from the SFO (for suspected fraud offences) and the EC (cartels and other anti-competitive behaviour), bodies empowered to carry out a dawn raid in the UK include the Office of Fair Trading, HM Revenue & Customs (tax offences), and the Financial Services Authority (insider dealing). The investigative powers of these bodies vary and, in some cases, will depend on the nature of the authorisation (or mandate) under which the raid is conducted.

However, investigators generally have the power to enter and search the premises of the target company (although not necessarily to do so forcibly) and request copies of documents discovered during the search.

Despite the term, dawn raids more usually take place during office hours, typically at the start of the working day. But in certain cases – notably investigations of criminal cartel activity – searches may take place earlier and be dawn raids in the literal sense. In the event of suspected criminal activity, the homes of employees may also be subject to the raids.

Clearly, the best preparation for a dawn raid is to ensure that compliance procedures are sufficiently robust to avoid regulatory breaches in the first instance. However, even if a company has no reason to suspect it might be guilty of any wrongdoing, it is still essential to prepare a dawn raid protocol on the assumption that a raid could take place at any time and without warning. These steps will include:

- circulating guidelines to employees that outline the powers available to the various authorities, provide information on the way in which raids are carried out, and set out a checklist of procedures that should be followed in the event of a raid
- briefing staff directly involved in dealing with a dawn raid – for example, receptionists, security staff and senior executives – on their individual responsibilities. Depending on the size and nature of the company, it may be worth extending this training programme to other employees, such as the IT department and in-house lawyers.

When the investigators arrive

Checking their mandate

On arrival, the investigators should produce their credentials and the authorisation for the raid. In the event of an SFO or Financial Services Authority (FSA) raid, this will be a warrant. The mandate should be checked to ensure that the investigators have the authority to carry out the raid. In particular, it is important to check that:

- the mandate applies to the company that is subject to the raid
- it is of a type to which the company is bound to submit
- the investigators are individually named in the mandate (or in an accompanying document)
- each investigator has valid identification
- the mandate was issued for a period that is still valid.

In competition investigations, the subject matter and period of the alleged infringement should be confirmed with the investigators and a note made of this. In inquiries by the FSA or SFO, the precise scope of the information required will be specified in the warrant.

Seeking a delay, but avoiding obstruction

It is advisable to request that the investigators delay their searches until in-house or external lawyers are present. In the event of a criminal raid, such a request is less likely to be granted; the Office of Fair Trading (OFT) and EC tend to be more willing to wait for a reasonable period, but this is unlikely to be more than an hour. As outlined above, it is important in this regard that front-line staff are adequately briefed to deal with the investigators if necessary.

It is, however, also important to note that an attempt to delay a search significantly may be construed by regulatory authorities as obstruction. That in itself may give rise to a fine, and it is a criminal offence to fail to comply with a lawful request made by the SFO during an investigation. In addition, there may be negative consequences in terms of any subsequent application for leniency in relation to a competition inquiry.

All staff, therefore, should be instructed to co-operate with investigators to the extent that the latter do not exceed the limits of their legal powers.

Monitoring the dawn raid

Shadowing

In general, investigators have the right to take copies of documents during their search. Certain regulatory authorities also have the right to take possession of original documents. It is crucial that each investigator is shadowed at all times by a company employee.

These 'shadowers' should make an additional copy of each document either retained or copied by the investigators, and also request a complete list of those documents from the investigators. Any questions asked by the investigator, as well as answers given, should be noted. A shadower should also ensure that no attempt is made to read or copy either 'privileged' documents or information that is not relevant to the scope of the inquiry.

Replying to questions

The rights of regulatory authorities vary in asking questions of employees during a raid. The OFT and EC are permitted to ask questions on the

location of relevant documents and request explanations of particular contents – for example, the meaning of internal codes. More general questions are not allowed and should not be answered; employees should take care to avoid self-incrimination or incriminating the company.

Although investigators generally have the right to ask to speak to any employee, a company should try to maintain a single point of contact for any questions – preferably an in-house lawyer or senior executive.

Other points to note

It is important not to inform anybody outside the company (other than external legal counsel) of the inspection, or to send internal emails commenting on the investigation, other than necessary instructions to staff.

In no circumstances should documents, whether electronic or hard copy, be destroyed once investigators have arrived. In the event an inquiry lasts for more than one day, the regulatory authorities may seal boxes or rooms; such seals should be well protected and staff should be instructed not to tamper with them.

In December 2010, the EU General Court upheld a fine of €38 million against a company for breaching an official seal following a dawn raid. Fines of up to 1 per cent of a company's annual turnover are permitted under EU law for such acts, and it is not necessary to prove by whom the seal was broken. Likewise, any destruction of a document that a person under investigation knows or suspects would be relevant to an SFO inquiry is a criminal offence.

Legal privilege and relevance

It is important that a company utilises its right of legal privilege during a dawn raid. The basic position under EU law (which will apply in the event of an EC raid) is that privilege covers confidential written communications between a company and external lawyers qualified in the European Economic Area (but not in-house lawyers), made for the purposes of the company's rights of defence. Under UK law, the position is more nuanced: privilege will generally apply to written communications with in-house lawyers and, broadly speaking, any legal communication created for the purpose of being used in actual or potential litigation.

The consequences of failing adequately to protect communications under legal privilege may be significant: in 2004 the EC fined Akzo Chemicals €21 million, having relied on incriminating communications between the company's in-house lawyers and various senior employees. The European Court of Justice upheld the fine, on the basis that in-house lawyers are not generally protected by legal professional privilege.

Employees should look to ensure that the investigating authority does not review documents that fall outside the scope of the mandate and are thus not relevant to the investigation. However, this is a judgement exercise; it may not be advisable to contest the relevance of borderline documents too strongly as this may be regarded as an attempt to obstruct the investigation. The final decision on relevance will be taken by the investigators, although it may be possible to redact irrelevant parts of a particular document.

Immediately following the raid

In practice, the steps that the company takes in the days after a dawn raid often have a significant bearing on the outcome of the case. The best course of action immediately following a raid will depend on the type of investigation involved and the specific facts at issue, but certain steps are necessary in response to any type of raid.

Assemble the right team

In larger organisations, there may be employees whose role would involve organising an internal investigation following a dawn raid. It is nevertheless crucial, given the potential impact on a company, to obtain appropriate external assistance. In terms of legal advice, since the initial stages of an investigation are of key importance in its eventual outcome, it is vital to select

experienced external counsel at the outset. It may also be necessary to obtain advice on handling the public relations consequences.

Ensure the retention of documents

A company that has been raided should immediately issue a 'document hold' and employee guidance on the retention of documents. It is critical that the company takes steps to ensure the preservation of all documents, data and other potentially relevant information, including electronically stored data, in order to avoid possible criminal penalties and jeopardising potential leniency applications.

Complete an initial internal audit

The company must immediately commence an expedited review of the evidence copied or confiscated by the authorities during the dawn raid. It is crucial to identify the salient facts regarding the alleged offence in order to be able to take the appropriate decisions on the best course of action. In particular, the company must take an initial view on whether there is any foundation for the allegations. An initial document review, possibly combined with brief interviews of relevant employees, will often be sufficient to formulate a working defence strategy.

Formulate a first defence strategy

Considerations relevant to all investigations

In most instances, a party's freedom of action in the immediate aftermath of a raid will be constrained by the authority's powers to demand explanations, document freezes and the production of documents from the raided party. In these circumstances, the most appropriate response is to obtain external legal advice immediately, both in order to start formulating a defence strategy and to ensure that the company is clear about its continuing obligations to the investigators and any relevant limits on their powers. For example, the SFO has ongoing investigatory powers that can be exercised on the same basis as when the initial raid took place, and any obstruction of these will also constitute a criminal offence.

Issues relevant to competition investigations

In the context of a competition investigation, the actions of the company in the immediate aftermath of a raid take on an even greater significance, since the severity of the sanctions for anti-competitive behaviour may be substantially mitigated in nearly all jurisdictions should a company choose to admit its role in a cartel and provide full evidence against itself at as early a stage in the investigation as possible. The fact of the dawn raid normally suggests that a participant in a cartel has self-reported and therefore assumed the 'immunity position'. There is, however, significant value in being 'second in' (a 30-50 per cent reduction in fines) as opposed to third (20-30 per cent reduction) or fourth (up to 20 per cent).

Cartel participants that have coerced others into participation will not be able to benefit from immunity in certain jurisdictions. It will, as a result, be important to quickly identify the role played by the company in a cartel.

The raiding authority will usually announce the dawn raid in the relevant sector within a few days, so alerting rivals that may look to approach the competition authorities. Responding quickly could make a difference. To minimise risk, a number of competition authorities may be contacted on an anonymous basis for guidance.

Certain jurisdictions allow a company to request a 'marker' to preserve an early-reporting time while the company performs a fuller internal investigation. The company must submit relevant evidence within the set period to 'perfect' this marker. Note, however, that a marker may be revoked only if the company fails to find evidence of an infringement, and not if it subsequently decides on a strategy of non co-operation.

Approaching local counsel in other jurisdictions

Many investigations lead to criminal and civil liability in multiple jurisdictions where a single set of facts amounts to an offence in those countries.

Under the Bribery Act, for example, companies may be liable for the act of bribery, the failure to prevent bribery and for the actions of their business partners wherever these take place, including where these partners are foreign companies.

Once a company has established those countries that may be affected, counsel should immediately contact experienced local counsel in those jurisdictions. The 'priority' areas include the EU (and member states), the US, Canada and Brazil – although Australia, Japan, New Zealand, Mexico and South Korea are increasingly active, in particular in competition enforcement.

Once a shortlist of 'hot' jurisdictions has been drawn up, the company will need to determine, in conjunction with local counsel, whether there is any value in approaching the relevant authorities to self-report the infringing behaviour in order to obtain formal or informal leniency in any future proceedings. For competition investigations, this shortlist will usually comprise the countries in which the alleged participants achieved sales; for other types of investigation, the relevant jurisdictions may be identifiable from the facts of the offence in question.

Conducting an internal investigation

Setting the scope of the investigation

The next priority is to determine the scope of the full internal investigation, and the physical location and custodians of the documents under investigation should be the starting point.

Non-competition investigations

For a raid involving potential criminal offences, it will be important to determine the individuals responsible (if any), and whether or not their seniority in the company, combined with any negligence in the compliance procedures and/or corporate behaviour, may lead to criminal sanctions against the company itself.

An appropriately focused internal investigation will identify any compliance-related failings, especially in a larger organisation, which may need to be remedied at the earliest opportunity to prevent any recurrence of the offence in question. It will also identify any ongoing offending behaviour that could aggravate the severity of potential sanctions.

It may be apparent to a company or individual subject to an investigation that an offence has not, in fact, taken place; if this is the case, the internal investigation must be prompt, thorough and appropriately targeted in order to mount as vigorous a defence as possible against any future charges.

Cost considerations may also come into play in determining the scope of an internal investigation; there may be limited value to a company in conducting an extensive and expensive inquiry if the relevant facts can easily be identified. In such circumstances, it may be worth adopting a more passive approach and simply responding to requests made by the authorities. It will be necessary to seek the guidance of external legal advisers in this regard.

Competition investigations

The scope of an internal investigation will often be far greater when a competition is the issue. In general terms, the investigation will need to catch the following:

- *Affected products.* The inquiry should focus in the first instance on the sector in which the raiding authority appears to be interested. It will be essential to understand the chain of distribution, the extent of sales (both direct and indirect) and the customers that may be affected.
- *The geographic scope of the alleged conduct.* The jurisdictions in which a cartel may have operated should be quickly identified. Any investigation flowing from the dawn raid will potentially draw the interest of competition authorities in other jurisdictions and, as described above, it may be possible to gain substantial discounts by voluntarily approaching thse authorities.
- *The duration of the alleged conduct.* The

investigation should determine the starting point of the alleged anti-competitive behaviour and whether there may have been any identifiable 'breaks' in such conduct.

- *The nature of the alleged conduct*. The investigation should assess whether the conduct involved geographic market allocation, price fixing, bid rigging or information exchange, the frequency of any meetings with competitors and the purpose of such contacts, and the specific role played by the company in a cartel.
- *Key employees for interview*. The individual role played by the relevant employees must be established. Witnesses should be interviewed separately and accurate notes recorded. The interviews should be carried out by external local counsel for the purposes of protecting legal professional privilege.
- *Other possible infringing conduct*. The inquiry should explore all anti-competitive behaviour with company employees – not just their knowledge of the products affected by the anti-competitive behaviour under investigation.

Managing the internal investigation

Although the internal inquiry should be set in motion as quickly as possible, the company must take care to assemble an independent team able to supervise the investigation across the relevant business units and jurisdictions. The company should also confirm whether there are any existing or concurrent investigations being carried out by other competition authorities. Co-operation and co-ordination between these enforcement authorities, often on an informal basis, should be expected.

Considering 'amnesty plus'

As described above, in the context of a competition investigation, the company's internal inquiry should extend to possible cartel activity in other sectors. This is particularly relevant in jurisdictions that have adopted the 'amnesty plus' programme, under which companies co-operating with the competition authorities may also report anti-competitive activity in related product markets in return for an amnesty for those markets. In the US, there may be negative consequences for a failure to do so, referred to as 'penalty plus'. The US competition authorities will probably ask witnesses about any other anti-competitive conduct of which they have knowledge – the so-called 'omnibus question'.

Next steps

Continued co-operation with the regulatory authorities

In the context of competition investigations, in order to qualify for immunity or a reduction in penalties, the company must continue to meet the conditions of the relevant leniency programme. It will be required to co-operate fully with the authorities, in particular by providing accurate and complete information. It will be further obliged not to disclose the fact or content of the leniency application and not to destroy, falsify or conceal relevant information or evidence relating to the alleged infringement.

A failure to comply with the conditions of the leniency programme will disqualify the company from the programme.

It is also likely that ongoing requests for the production and/or explanation of documents and other information will be made by the authorities; responding to these will be crucial, as not to do so may hinder a leniency application and, in certain circumstances, constitute a criminal offence.

Employee management issues

A company will need to consider certain staff-related issues following a dawn raid, including applicable employment law and data protection rules. For example, the company may need to obtain an employee's consent for the transfer of his or her personal data outside the European Economic Area, where the third country may not ensure an adequate level of protection.

In addition, it will be essential to resolve any

conflicts of interest between individual staff members and the company. For example, some employees may require separate legal representation in certain jurisdictions, such as the UK and the US, depending on the alleged conduct.

A company may also need to consider whether disciplinary action may be appropriate. Often, investigating authorities will expect individuals involved in unlawful or criminal behaviour not to be promoted subsequently, and may even wish to see them demoted or even dismissed in the context of a formal or informal co-operation programme.

Accounting and disclosure issues

A company may also want to consider including provisions in its accounts to reflect its potential financial exposure to sanctions and/or civil litigation.

Bespoke compliance programmes

A company should also review and update (or put in place) compliance programmes in order to reduce the chance of recidivism. The nature and extent of the programme may depend on the size of the company, the relevant sector and the background of the employees, but it will often include the circulation of a detailed compliance manual, together with regular training sessions and interactive tools.

Preparing for civil damages actions

The potential for civil damages actions will depend on the alleged offence under investigation. But where it could have a significant negative effect on a listed company's share price, for example, the company's own shareholders may contemplate civil actions for damages against the management.

In the context of anti-competitive conduct, in particular, there is a significant risk of private litigation. Although, historically, that danger has been confined to the US, other jurisdictions are in the process of establishing effective legal frameworks for such actions. In addition, in the EU, a final EC infringement decision will be binding on national courts in member states and may give rise to 'follow-on' actions.

A company must therefore secure and review all documentary evidence in its originating jurisdiction to protect against the risk of discovery in any future foreign proceedings. A company should take care to check the location of servers used to host related documents.

Conclusion

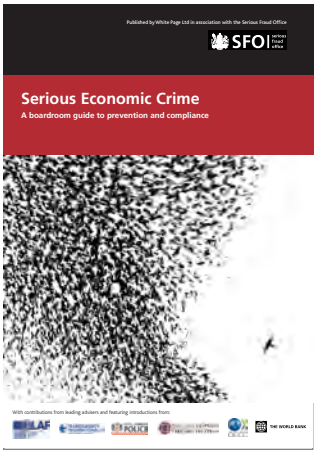
The steps taken by a company in the days and weeks following a dawn raid will often have a major bearing on the strategic choices subsequently open to the company. The difference between getting the strategy right and getting it wrong can usually be measured at the end of any lengthy investigation.

Winston & Strawn LLP
City Point, One Ropemaker Street
London EC2Y 9HU
Direct Tel: +44 (0)20 7011 8750
Fax: +44 (0)20 7011 8800
Web www.winston.com

Peter Crowther
Partner
Email PCrowther@winston.com

Mr Crowther defends companies in a wide range of national and international government and regulatory enforcement proceedings, often simultaneously across jurisdictions. He also devises and implements compliance programmes covering such areas as competition, trade/sanctions, and bribery and corruption.

Mr Crowther is a former law lecturer and former holder of a Jean Monnet Professorship in European Law. He was named one of *The Lawyer*'s 'Hot 100' for 2011.



Published by White Page Ltd in association with the Serious Fraud Office, Serious Economic Crime's primary purpose is to give board-level readers in the UK and international businesses informed commentary on the impact of UK anti-fraud and anti-corruption legislation. As the scope of this legislation continues to expand and interact more with the legislation in other jurisdictions, so the landscape for best-practice compliance and fraud prevention has become increasingly complex. The wealth of expert insights from lawyers, accountants and specialist anti-fraud consultants in this publication's 36 chapters is therefore an invaluable resource.

This publication is written as a general guide only. It should not be relied upon as a substitute for specific legal or other professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in the articles contained in this publication are those of the authors. They do not necessarily reflect the views of the Serious Fraud Office and should not be taken as endorsed by the Serious Fraud Office. The publishers and authors bear no responsibility for any errors or omissions contained herein.

To view the book in which this chapter was published, to download iPad and Kindle-compatible editions and/or to order hard-copy versions, please go to www.seriouseconomiccrime.com

Published by White Page Ltd www.whitepage.co.uk