# TABLE OF CONTENTS

INTRODUCTION TO DAWN RAIDS

ACTION PROTOCOL: DEALING WITH DAWN RAIDS

A. First Steps

B. The Search

C. Privileged Documents

D. Penalties

MEETING WITH THE INVESTIGATORS AT THE END OF THE DAY

AFTER THE RAID

ANNEX 1 - RELEVANT AUTHORITIES AND THEIR INVESTIGATORY POWERS

ANNEX 2 - ENTERING THE PREMISES AND SCOPE OF SEARCH
Any company, regardless of its size, may be subject to a “dawn raid.” Dawn raids are surprise investigations of premises and are usually without warning.

The prospect of dawn raids has become a reality for many businesses. It is important to know how to handle a dawn raid and to have a response procedure in place, both to ensure that the company fulfils its legal obligations and to ensure that the company’s legal rights are respected. It is also important to minimise the impact of the raid on the company’s day-to-day business and reputation.

Many authorities have the power to search and gain entry to premises without notice and to make arrests. Ensuring that your organisation has a protocol for dealing with a visit by one of these authorities and that staff are aware of the existence and content of your dawn raid policy is crucial.

This guide will consider the key practical points and legal issues to bear in mind when facing a dawn raid. This guide should be used to assist your company in providing an effective response in the event of a dawn raid. This guide does not act as legal advice and should not be relied on as such.

K&L Gates’ Government Enforcement team is available to answer any queries about the impact of dawn raids on your clients’ businesses or to attend businesses’ premises in the event of a dawn raid.
FIRST STEPS

The first people to face investigators from the raiding authority will, most likely, be the receptionists. It is important that the receptionists have clear instructions of how they are to proceed and whom they should alert.

Everyone should remain calm and cooperate with the investigation. You will be presented with a warrant or decision notice providing details of the scope of the search and the reasons for the search. Once it has been ascertained that the raiding authority has the authority to conduct a search of the premises, you should bring the investigators to an empty meeting room or other secure area away from common areas.

Establish how many locations are subject to the raid and consider the number of representatives needed at each location. You should immediately contact:

- senior management;
- in-house legal or compliance representatives; and
- your external counsel

to attend the premises as soon as possible.

While the raiding authority will allow you to call your external counsel to attend the search, they are under no duty to suspend their investigation until counsel arrive. However, it is usual for the raiding authority to accept a short delay before commencing their search of the premises. Therefore, you should make this request upon identification of the investigator in charge of the dawn raid.

Explain to any staff aware of the investigation that they must not discuss the investigation except where expressly authorised to do so.

It is highly recommended that you issue an instruction that no shredding of documents or deletion of electronic materials is to take place on the day of the dawn raid until further notice.

THE SEARCH

On arrival of senior management, legal or compliance representatives and external counsel (your “dawn raid team”), an attempt should be made to agree upon an approach with the raiding authority by which the search can take place with the least interference with the day-to-day operation of the business. The inspectors from the raiding authority are likely to ask for clarification on the internal organisation of the company, its business areas, IT systems, and general layout of the building.

The dawn raid team should take the following steps:

- Obtain copies of the warrant, if not already available, and review it for validity, scope, and key terms;
- Inform the raiding authority that requests for oral explanations should be directed to designated point(s) of contact, whether the office head, the head of compliance, the relevant regional business group heads, senior legal or compliance representatives, or external counsel;
- Ensure that the investigation is appropriately supervised by having one or two members of the dawn raid team shadow each inspector from the raiding authority. Do not allow inspectors to roam freely around the offices, and make sure that their search is restricted to the terms of the search warrant. Each inspector should be accompanied at all times, and a written record should be prepared reflecting which areas were visited; what desks, cupboards, files and computers were examined; and any questions asked and answers given.
- Any specific documents and records requested by inspectors must be produced by the company.¹ It is very important to take a full note of what items or documents are taken by the raiding authorities, including electronic materials and computers. The

¹ Case 374/87 Orkim v Commission [1989] ECR 3283, paragraph 27
investigators may be entitled to take originals (this will be determined by the terms of their warrant), in which case copies should be made of every document taken by the investigators, if possible (there is no right to do so).

Investigators will usually be looking for:
- minutes and notes of meetings;
- internal reports;
- correspondence (emails and letters);
- personal diaries (physical or electronic form);
- sales, invoices, and pricing data;
- travel records;
- personal notebooks and papers; and
- computers, mobile phones, USB devices, and tablet devices.

The investigators may ask questions of any staff and request that they provide factual replies. Any questions that go beyond seeking factual clarification are not permitted. As the investigators’ questions could be directed at anyone and not just those identified by the dawn raid team, all staff should be aware to provide specific, truthful and factual replies but offer no extra detail.

The investigators are entitled to seal rooms or cabinets overnight, disconnect electronic equipment, or temporarily block individual email accounts during an investigation. Full cooperation should be given to assist inspectors, and these seals must not be disrupted.

PRIVILEGED DOCUMENTS

It will be necessary early on in the course of the investigation to identify any documents protected by legal privilege and put them to one side so as to avoid accidental disclosure to the inspectors.

In relation to an investigation by the European Commission, written communications will be privileged if they are:
- made between the company and an independent external lawyer qualified to practise in an EEA Member state (i.e., excluding in-house lawyers and, for example, U.S. lawyers); and
- made for the purposes of, and in the interests of, the client’s rights of defence in relation to the investigation.

If the CMA is ‘acting on behalf of’ (s63 Competition Act 1998) rather than ‘assisting’ the European Commission, it will apply the UK rules on privilege. The CMA is deemed to ‘assist’ when the European Commission are carrying out the inspection and the CMA is present with a warrant (s62 Competition Act 1998) in case there is any likelihood of obstruction by the company.

If the CMA is carrying out an inspection on its own behalf (s27 Competition Act 1998) or carrying out an inspection on another member state’s behalf (s65F & G Competition Act 1998), UK rules of privilege will apply.

UK rules surrounding privilege cover a wider category of communication than EU law. In particular, UK law extends privilege to communications with in-house lawyers and privilege is not restricted to matters relating to the client’s rights of defence. Privilege arises in two instances:
- legal advice privilege:
  - the relevant communication must be confidential between client and lawyer (including in-house lawyers); and
  - the relevant communication must be made for the purpose of giving or seeking legal advice.
- litigation privilege:
  - the relevant communication must be confidential between client or its lawyer (including in-house lawyers) and the sender/recipient; and
  - the relevant communication must have come into existence for the dominant purpose of being used in contemplated or pending litigation.

Any document that benefits from privilege should not be disclosed. It will, however, be necessary to provide an explanation as to why the documents are privileged, which could be done by:
- disclosing the heading or certain passages of the document;
- producing other documents referring to the disputed document; or
- making a formal statement as to the nature and content of the documents.

If there is a dispute as to whether a document is privileged, an attempt should be made to put the document to one side or to hold it separately in a sealed envelope pending later determination by an independent party. This will avoid delaying the investigation.
In relation to the seizure of electronic material, there will usually be privileged material of some sort on company computers and servers. This could include legal advice relating to contract negotiations, employment disputes, commercial litigation, etc. Do not be afraid to say that you believe there is likely to be privileged material on electronic devices or within electronic material being seized. Similarly, computers and servers will store material that is irrelevant or in any event not responsive to the warrant. The usual approach is that computers and servers will be taken and copied off-site prior to being searched by the relevant authority, although some authorities may be convinced to copy computers and servers on-site prior to leaving the premises so as not to disrupt business activity.

If documents contain business secrets but are not privileged, the investigators are entitled to access to the material but will be subject to restrictions when considering disclosure of such material to third parties.

PENALTIES

If an individual resists or obstructs the raiding authority during the course of their investigation they may be guilty of an offence.

Any attempt to destroy or hide any documents could also amount to perverting the course of justice. The offence is committed where a person acts or embarks in a positive way on a course of conduct that has a tendency to and is intended to pervert the course of public justice.

The CMA

If a company fails to comply with the CMA’s investigation, they could be liable to pay substantial fines.

It is a criminal offence for a person to:

- obstruct an officer carrying out an on-site investigation (even if not under warrant) intentionally;
- destroy, falsify, or conceal a document that is requested by the CMA, knowingly or recklessly; or
- provide false or misleading information to the CMA, knowingly or recklessly.

These offences are punishable by fines or, in certain cases, imprisonment of up to two years, or both.²

If any of these offences is committed by, with the consent of, or as a result of the negligence of a director, manager, or other similar officer of a company, the company will also be guilty of the offence.

The European Commission

The European Commission may impose a fine of up to 1% of group turnover where a company:

- produces incomplete books or records or refuses to produce books or records³;
- refuses to answer a question relating to facts or documents relevant to the inspection⁴ and;
- breaks seals placed on documents or premises by inspectors⁵.

An additional penalty of up to 5% of the average group daily turnover may also be imposed for each day the company refuses to permit an inspection.⁶

A company will have the right to be heard by the European Commission before any fines are imposed.

The SFO

If a company or individual fails to cooperate, it becomes liable to criminal prosecution and penalties under section 2 of the Criminal Justice Act 1987.

This section states that:

- any person who fails (without a reasonable excuse) to comply with the requirements imposed on him by the SFO shall be guilty of an offence punishable by up to 6 months in prison and/or a fine up to £5000⁷;
- any person who makes a statement to the SFO (under the section), which he knows to be false or misleading, or recklessly makes such a statement, may be guilty of an offence punishable by up to 2 years in prison and/or a fine⁸; and
- any person who knows or suspects that an investigation is likely to be carried out and falsifies, conceals, or destroys documents that are known or suspected to be relevant to the investigation shall be guilty of an offence punishable by up to 7 years in prison and/or a fine.⁹

² s65 Competition Act 1998, s. 201 Enterprise Act 2002.
³ Article 23(1)(c) Regulation 1/2003.
⁴ Article 23(1)(d) Regulation 1/2003.
⁵ Article 23(1)(e) Regulation 1/2003.
⁷ s2(13) CJA 1987.
⁸ s2(15) CJA 1987.
⁹ s2(17) CJA 1987.
**The FCA or PRA**

The intentional obstruction of an investigation amounts to a criminal offence under s. 177(6) FSMA.

If a company fails to comply with their duty to cooperate under Principle 11 of the Principles for Business (PRIN) the company may be subject to enforcement proceedings by either the FCA or the PRA, which could result in an unlimited fine.

**The Police**

Any person who obstructs a police officer from carrying out their investigation shall be guilty of an offence punishable by imprisonment, a fine, or both.\(^{10}\)

**HMRC**

Any person who fails to comply, without reasonable excuse, with the requirements imposed on him by SOCPA or any person who obstructs an investigation under a SOCPA warrant will be guilty of an offence punishable by up to 51 weeks’ imprisonment and/or a fine of up to £5,000.\(^{11}\)

Any person who makes a statement in response to a request under SOCPA which he knows to be false or misleading, or recklessly makes such a statement, may be guilty of an offence punishable by up to 2 years in prison and/or a fine.\(^{12}\)

**The HSE**

Intentionally obstructing or failing to comply with an investigator under HSWA is a criminal offence punishable by a fine of up to £5,000 and/or up to 51 weeks’ imprisonment.\(^{13}\)

---

\(^{10}\) s89(2) Police Act 1996.

\(^{11}\) s67(4) SOCPA.

\(^{12}\) s67(5) SOCPA.

\(^{13}\) s33 HSWA.
A meeting should take place between the investigators and the dawn raid team at the end of the day. During this meeting you should establish:

- whether the investigation will continue into the following day and, if this is the case, whether the investigators require certain areas to be sealed overnight;
- which business sites will continue to be involved (this is particularly relevant where a number of premises have been raided) and at what time the investigators will be returning;
- whether there are any documents subject to dispute as to whether they may be copied and/or seized and consider any arguments made to persuade the regulator that the documents are irrelevant or privileged.

A record of the dawn raid will likely be drawn up by the raiding authority, including an inventory of the documents seized and a record of the questions asked. The leading member of the dawn raid team should:

- read the document carefully;
- ask to make any corrections and/or additions;
- make notes of any statements in the record with which you disagree;
- include notes of any difficulties encountered with the authority during the investigation;
- ask for a copy of the document; and
- if requested to sign the record, refuse to sign it if it does not correspond with what has been taken and that person has not been allowed to make any desired change(s).
Once the investigators have left the premises, the following steps should be a priority:

- arrange a meeting with the office head; the head of compliance; any relevant business group heads; relevant business legal or compliance representatives; external counsel; human resources; corporate communications; and the head of IT to discuss strategy for dealing with the investigation;

- discuss in the strategy meeting whether any further explanations or documents need to be provided to the raiding authority;

- prepare the team for a follow-up visit at a later stage or any follow-up requests by the investigators for information by telephone or letter, and ensure that relevant staff are briefed of this possibility;

- suspend any routine document destruction policy and prevent electronic documents from being deleted, which may involve increasing mailbox limits to prevent the automatic deletion of emails and suspending automatic processes that erase or replace electronic data;

- identify any individuals suspected of involvement and, in most cases, remove them from their usual duties and/or suspended them as soon as is practicable in accordance with employment law;

- prepare a precise and fact-based written report of the raid as soon as possible, while the events are fresh in the mind;

- avoid making any personal commentary on the raid in writing or by telephone;

- ensure that anyone who is arrested has proper legal representation at any interview under caution;

- seek advice on the existence of any reporting obligations, for example, under stock exchange rules;

- if necessary, notify insurers; and

- if necessary, prepare a short, agreed statement which can be released publicly in the event that the company is approached by the press; the statement need not say any more than that the company had been visited by the raiding authority and that it is cooperating with the investigation. It is advisable that any such statement be drafted with legal counsel and approved by a senior member of the management team.

Depending on the nature of the investigation, the company may consider undertaking its own broader internal investigation to ascertain whether the company has exposure. A dialogue with the authority should be maintained throughout the process; importantly, the authority may require that its approval is sought to any investigation or terms of the investigation. In order to preserve legal professional privilege in the conduct of this investigation, legal counsel should be closely involved. A protocol should be drafted to govern the treatment of any sensitive or privileged material created by the internal investigation.

If the raiding authority concludes that any documents seized are irrelevant then they will be returned to the company. Any documents not returned as irrelevant will be placed on an ‘investigation file.’
In the UK, dawn raids and other visits or inspections may be undertaken by:

- the Competition and Markets Authority (“CMA”);
- the European Commission;
- the Serious Fraud Office (the “SFO”);
- the Financial Conduct Authority (the “FCA”) (formerly, the Financial Services Authority) and the Prudential Regulation Authority (the “PRA”);
- the Police;
- HM Revenue and Customs (“HMRC”); and
- the Health & Safety Executive (the “HSE”).

**THE CMA**

Under the Enterprise and Regulatory Reform Act 2013 the CMA took over all competition functions of the OFT and Competition Commission. As a result the CMA has the power to enter both business and domestic premises in relation to competition investigations under the Competition Act 1998 and criminal investigations under the Enterprise Act 2002. The CMA may also carry out inspections on behalf of another member state’s competition authority and assist with or conduct an investigation on the EU Commission’s behalf. When the CMA has reasonable grounds for suspecting that there has been a breach of EU or UK competition rules, the powers available to it include:

- the ability to compel an individual or company to provide documents (Production Order);
- the ability to compel any individual connected with a business that is party to an investigation to answer questions about a document;
- the ability to enter a business premises with or without a warrant if the premises are used for business or documents are kept there; and
- the ability to examine and take copies of documents or information held on a computer.

If the CMA wishes to conduct a dawn raid on a company that is not itself the subject of the investigation, it must give two working days’ notice and indicate the subject matter and purpose of the investigation and the nature of the offences under investigation.

Under the Enterprise Act 2002 the CMA may make an application to the High Court for a warrant to search business and domestic premises where they are investigating a criminal cartel and reasonably believe that a person has failed to comply with a production order or where it is not practicable to serve a notice requiring the production of documents.

**THE EUROPEAN COMMISSION**

The European Commission has the power under Regulation 1/2003 to investigate possible infringements of EU competition law.

The European Commission can carry out investigations under Regulation 1/2003:

- pursuant to written authorisation; or
- pursuant to a formal European Commission decision.

The type of investigation being carried out by the European Commission will be made clear on the documents presented by the inspectors on arrival at the company’s premises. If the investigation is by authorisation only, the company is not obliged to comply but is asked to submit to the investigation voluntarily. It is usually advisable for the company to submit to the investigation voluntarily as the investigators can quickly convert an authorisation to a formal decision. If a...
company does not comply with a formal decision, fines can be imposed.

Officials from the CMA will usually accompany inspectors from the European Commission, and they may have also obtained a search warrant, which may be executed if a company obstructs the European Commission’s investigation.

THE SFO

In general, the SFO will investigate serious or complex frauds and corruption that often involve an international element or are likely to attract publicity. In doing so, the SFO has statutory powers to:

- compel persons to answer questions;
- compel persons to produce documents for the purpose of an investigation, or alternatively;
- search property.

S2 of the Criminal Justice Act 1987 (“CJA 1987”) gives the SFO the power to require a person to provide information either by producing material or attending an interview. Alternatively, the SFO may search premises. This power may only be used when the Director of the SFO finds reasonable grounds to suspect that an offence that involves serious or complex fraud or corruption has been committed. The SFO always provides written notice when exercising this power, explaining the need for an officer to attend the premises of the company. The SFO can also use powers under POCA to obtain search and seizure warrants, in relation to specific types of investigation.

Alternatively, where there is concern that documents may be either lost or destroyed, the SFO may conduct dawn raids without notice. In almost all cases, the SFO will conduct raids with the police. In these cases the SFO usually seeks a court warrant allowing them (while accompanied by a constable) to enter premises and to search and seize relevant evidence. The police have a general power of seizure once on premises lawfully.

The SFO maintains memoranda of understanding between themselves and many other agencies, which memoranda set out the basis of each authority’s cooperation in investigating cases.

THE FCA AND PRA

The FCA regulates financial firms providing services to consumers and maintains the integrity of the UK’s financial markets. It focuses on the regulation of conduct by both retail and wholesale financial services firms. The PRA is responsible for the prudential regulation of PRA-authorised firms (broadly, deposit takers, insurers, and designated investment firms).

The powers under The Financial Services and Markets Act 2000 (“FSMA”) referred to in this note are exercisable both by the FCA or the PRA.

The FCA/PRA’s powers are found in FSMA and allow its officers to:

- obtain warrants and enter the premises of businesses;
- request the production of documents; and
- compel the attendance of individuals to provide documents and/or answer questions.

The FCA’s Enforcement Guide (“EG”) provides a summary of the FCA’s legislative powers and gives guidance on the factors that influence the decision as to whether to use these powers and on the basis upon which investigations will be conducted.

The FCA generally investigates market abuse, breaches of its rules, insider dealing, criminal offences under FSMA, and money laundering, although, depending on the nature of the offence, the police, SFO, and National Crime Agency (“NCA”) may also investigate these offences.

THE POLICE

The majority of offences in England and Wales are investigated by the police.

The Police and Criminal Evidence Act 1984 (“PACE”) governs the issue and execution of search warrants and of court orders for production and access to records. Investigators may seek warrants to seize “special procedure material” (papers held under a duty of confidentiality) or excluded material (which includes personal records and journalistic material). In cases where a warrant is granted under

---

26 See: http://www.sfo.gov.uk/our-work/our-cases/historic-cases.aspx
32 See: [MISSING FOOTNOTE]
34 s19 PACE: http://www.legislation.gov.uk/ukpga/1984/60/part/1/crossheading/seizure-etc
Schedule 1 of PACE, is properly certified and clear in its scope, only material covered by legal professional privilege may be withheld.

The police also have extensive document production, disclosure and warrant execution powers under the Proceeds of Crime Act 2002 (“POCA”). The police have the power to seize cash and property that is suspected of being the proceeds of crime, and exercise powers of search and seizure under POCA. It must be the police who exercise these powers on behalf of the HMRC in relation to direct tax offences.

A number of additional powers of production and disclosure of electronic material are contained in the Regulation of Investigatory Powers Act 2000 (“RIPA”). Under RIPA the police can access protected data. More commonly, seized data from a production order under schedule 1 of PACE may be protected by a form of security measure, such as a password or cryptographic mechanism, which makes the data unintelligible. RIPA provides that once certain conditions are met, a notice may be served on a person to disclose the protected information in intelligible form.

Police have the power to issue a disclosure notice to a third party under The Serious Organised Crime and Police Act 2005 (“SOCPA”) if it appears that there are reasonable grounds for suspecting that an offence has been committed; that information to which the matter relates exists; and that there are reasonable grounds for believing that the material provided by the third party is likely to be of substantial value. Police also have the power to enter premises and seize documents under SOCPA if a disclosure notice is not complied with or it is not practicable to give a disclosure notice requiring document production.

Additional powers of seizure relating to electronic data are given to police under the Criminal Justice and Police Act 2001 (“CJPA”).

HMRC

The powers of HMRC to obtain information and inspect premises are derived mainly from PACE, POCA, the Finance Act 2008 (“FA”), and SOCPA.

The Finance Act 2007 amended PACE for all HMRC criminal investigations. Therefore, PACE provides search and seize powers, production order powers, arrest powers, and search and entry powers to arrest to HMRC when investigating tax frauds.

Schedule 36 of FA gives HMRC the power to request production of documents from a party and from third parties where HMRC wishes to check the tax position of that person or business.

SOCPA confers powers on the HMRC to request documents and information from persons who may have information relevant to tax-related crimes.

THE HSE

The Health and Safety at Work etc. Act 1974 (“HSWA”) gives a wide range of powers of investigations into incidents of noncompliance with health and safety law.

HSE inspectors appointed may:

- enter any premises for the purposes of enforcing HSWA;
- require the production of documents;
- take samples and measurements to assist the investigation; and
- require individuals to answer questions and sign a declaration of the truth of the answers.

There may be certain instances in which both the Environmental Agency and the HSE have the power to investigate an incident, and in such cases a Memorandum of Understanding will require the two regulators to work together and share information.

---

38 s8 – 16 PACE: http://www.legislation.gov.uk/ukpga/1984/60/contents
39 Schedule 1, PACE: http://www.legislation.gov.uk/ukpga/1984/60/schedule/1
42 s49(2) and s49(3) RIPA: http://www.legislation.gov.uk/ukpga/2000/23/part/III
46 s50 and 51 CJPA: http://www.legislation.gov.uk/ukpga/1984/60/schedule/1
47 s8 – 16 PACE: http://www.legislation.gov.uk/ukpga/1984/60/contents
ENTRY WITHOUT A WARRANT

Apart from the instances indicated below, a raiding authority has no legal power to forcibly enter premises or to seize any original documents without a court warrant.

The European Commission and the CMA may conduct a dawn raid on a suspected company without a warrant but their powers are limited to:

- requiring the production of documents or information, irrespective of the medium on which they are stored\(^\text{58}\);
- requiring connected individuals to answer questions\(^\text{59}\); and
- taking reasonable steps to prevent interference with any documents, e.g., by applying seals.

In limited circumstances a police officer may enter and search premises without a warrant:

- under s17 PACE, a police officer may enter and search any premises for the purpose of:
  - executing a warrant of arrest;
  - arresting a person for an indictable offence; or
  - in other specified circumstances (not applicable to most dawn raids upon businesses); and
- under s18 PACE, a police officer is permitted to enter and search any premises occupied or controlled by a person who is under arrest for an indictable offence if he has reasonable grounds for suspecting that there is on the premises evidence that relates to that offence or to some other offence that is connected with, or similar to, that offence.

If a formal investigation has commenced, other authorities may serve a document request requiring specific documents to be produced at a specified time and place. The document request imposes a duty on the recipient to provide the investigator with the relevant documents. In practice, the recipient has the right to a reasonable period to gather the documents and provide them to the appropriate regulator; although there has been a recent increase in the number of “here and now” production orders to combat the potential destruction or falsification of documents. If the recipient fails “without reasonable excuse” to comply with the document request, that appropriate regulator could apply to the court to hold the recipient in contempt of court.

ENTRY WITH A WARRANT

Before commencing an inspection, the raiding authority must present a warrant or other authorisation document stating the subject matter and purpose of the investigation.

Warrants provide those conducting the dawn raid with additional powers, such as the ability to use reasonable force to gain entry.

It should be noted that it is a criminal offence to intentionally obstruct the exercise of rights conferred by a warrant\(^\text{60}\) (see penalties section on page 6).

The search warrant may be obtained from the Crown Court, the High Court, or the Competition Appeal Tribunal. The warrant may be obtained in circumstances where:

- a person on whom an information request has been served has failed to comply with it; or
- there are reasonable grounds to believe that:
  - an information request would not be complied with; or
  - the documents or information to which the document request related would be removed, tampered with, or destroyed.

The entry and search must be exercised within three months of the date of issuance of the warrant by the court and should be exercised within reasonable hours unless it appears to the raiding authority that the purpose of the search may be frustrated by entry at a reasonable hour\(^\text{61}\).

Where the occupier of the relevant premises is present, the raiding authority must identify themselves to the occupier and produce identification. The raiding authority must also

---


\(^{60}\) s177(6) FSMA, s. 2(4) CJA 1987, s.89(2) Police Act 1996, Articles 23 - 24 Regulation 1/2003.

\(^{61}\) s16 PACE.
produce the warrant for entry and supply a copy of the warrant.\textsuperscript{62} All copies of the warrant should be clearly certified as copies.

\textbf{THE WARRANT}

A warrant should specify:

- the name of the person who applied for it;
- the date on which it is issued;
- the authority under which it is issued;
- each set of premises to be searched;
- in the case of an “all premises” warrant, the person who is in control or occupation of the premises to be searched and any premises that can be specified and can be searched; and
- so far as practicable, the articles or persons sought.

If the application is for an all-premises warrant, there must be reasonable grounds for believing that it is necessary to search premises not specified in the application in order to find the relevant material. It must not be reasonably practicable to specify in the application all of the premises that is occupied or controlled and might need to be searched.\textsuperscript{63}

Additional information should be given to the occupier or controller of the premises, which information sets out their rights and warns that destruction of information may amount to an offence, as it could prejudice the investigation.

\textbf{FSMA WARRANT}

A court warrant may be obtained by the FCA and the PRA in the limited circumstances described in s176 of FSMA.

A warrant issued by the court under s176 of FSMA will authorise the investigators to:

- enter the premises using such force as may be reasonably necessary;
- search the premises;
- take possession of documents or information appearing to be relevant;
- take copies or extracts from any such documents or information;
- require any person on the premises to provide an explanation of any document or information; and
- require any person on the premises to inform the investigators where a document may be found.

\textbf{POCA WARRANT}

A POCA warrant must be obtained from a Crown Court Judge (for confiscation or money laundering investigations) or a High Court Judge (for a civil recovery investigation).

In addition to the reasons given at Annex 2 (b) above, a warrant may be granted by the court if the conditions set out in s353 POCA are satisfied. This section provides that, in the first instance, there must be reasonable grounds for suspecting that:

- in the case of a confiscation investigation, a person specified in the application for the warrant has benefited from his criminal conduct;
- in the case of a civil recovery investigation, the property specified in the application for the warrant is recoverable property or associated property; or
- in the case of a money laundering investigation, the specified person has committed a money laundering offence.

In addition, there must also be reasonable grounds for believing that:

- the material on the premises specified in the application is likely to be of substantial value to the investigation;
- it is in the public interest for the material to be obtained having regard to the benefit likely to accrue to the investigation if the material is obtained; and
- it would not be appropriate to make a production order because it is not practicable to do so, or the investigation would be seriously prejudiced.

\textsuperscript{62} s16 (5) PACE, PD 8.1 Application for a warrant under the Competition Act 1998.\textsuperscript{63} The warrant may authorise an appropriate person to use force as is reasonably necessary (s. 66(3)(a) SOCPA).
SOCPA WARRANT

Under s. 66(1) of SOCPA, a warrant may be issued by the court when an oath is given by a member of the investigating authority (e.g., the Director of Public Prosecutions or the Director of Revenue and Customs Prosecutions) authorising a named appropriate person (a member of the CMA, a police officer, member of the NCA, an officer of HMRC) to undertake the raid with the additional powers of a warrant.\textsuperscript{64}

The court will grant the warrant if the conditions stated in Annex 2 (b) above are satisfied and there are reasonable grounds for suspecting that one of a number of offences has been committed.\textsuperscript{65} These offences include money laundering, counterfeiting, blackmail, bribery, and/or corruption.\textsuperscript{66}

The raiding authority may carry out their investigation with the assistance of local police forces, which may provide them with additional police powers. Reference should then be made in the additional information provided with the warrant to the police powers section and powers contained under the PACE.

\textsuperscript{64} s61 (1) SOCPA.

\textsuperscript{65} For a full list of offences see s.61(1) of SOCPA: a) Any offence listed in Schedule 2 of the Proceeds of Crime Act 2002 (lifestyle offences, e.g., money laundering, counterfeiting, blackmail); b) Any offence under sections 15-18 of the Terrorism Act 2000 (e.g., offences relating to fund-raising, money laundering); c) Any offence under section 170 of the Customs and Excise Management Act 1979 (fraudulent evasion of duty) or section 72 of the Value Added Tax Act 1994 (offences relating to VAT); d) Any offence under section 17 of the Theft Act 1968 (false accounting) or any offence at common law of cheating in relation to the public revenue; e) Any offence under section 1 of the Criminal Attempts Act 1981 (attempts); f) Any offence under section 1 of the Criminal Law Act 1977 (conspiracy), and g) Bribery and/or corruption.