Preparing for Search and Seizure Visits

This document is to be read in conjunction with the document entitled 'Search and Seizure: Information for officers'. Together, the documents assist employees and company officers in understanding what to do in the event of a 'raid' by HMRC and/or the police in the execution of search warrants at premises or vehicles at premises.

This document is not a substitute for legal advice. Different businesses will have individual requirements and you should contact JMW directly to discuss your needs, rather than simply implement what you see below.

Contact
Evan Wright: Partner
JMW Solicitors
0345 872 6666
www.jmw.co.uk

Background

Perhaps the most disruptive intervention for any business is the concept of a Dawn Raid. They typically occur early in the morning and are carried out by law enforcement officers when they believe that an unannounced visit is the only effective way to gather evidence.

It does not necessarily mean that persons at the premises are under investigation (although this is often the case). It may only mean that a search warrant was obtained because the officers believe the premises holds information relevant to the investigation. For example, this sometimes occurs where officers obtain a warrant to search an accountant's office for papers belonging to a client company, when the accountant's firm itself is not under suspicion.

In most cases, officers will arrive at the premises with a warrant granted by a Crown Court judge. The judge will have been provided with a statement of information setting out why the officers think a warrant is necessary and why, for instance, the evidence cannot be obtained by simply asking the subject to provide information in correspondence. Consequently, the obtaining of the warrant is confirmation that the premises may be searched without notice and obstructing the officers can amount to a criminal offence punishable by imprisonment.

Some search and seizure operations are very complex and involve dozens of officers in gathering information over the course of hours or even days at the subject premises. Large operations often appear chaotic and quite often lack structure or proper supervision. Persons at the premises will often feel that they have already been found guilty of something. It is therefore important to understand what the officers can and cannot do in the proper execution of their duties.

You should be assertive and you should not take assurances at face value. Ensure that if an officer promises to provide something during the search, or subsequent to the search, you obtain good contact details and a note of what was promised. However, there is a fine line between being assertive and obstructive. Professional officers will respect your rights and will assist where possible. Officers with a different agenda may allege that you are being obstructive so that they can go about their business as they want to, not necessarily in accordance with the law. It is important to ask why the relevant officer thinks that you are being obstructive and record the allegation.

Officers should be told that a little extra time invested at the start in getting the search and seizure correct almost always saves more time later in the exercise. It often avoids the need for disclosure applications and, in some instances, judicial review.

Responsible businesses prepare for this eventuality because the consequences of a raid can be far reaching. Many HMRC raids are in respect of matters that do not proceed to prosecution against the subject company, but the opportunities to claim damages against HMRC as a result of a raid without further action are very limited. Raids can have a dramatic impact on profitability and it may be said that a company is under a duty to mitigate potential damage.

Overview

1. Nominate a person to liaise with the officer in charge of the visit
2. Ask Officers to Produce Their Identification
3. Notify Your Solicitor
4. The Warrant
5. Shadow and Record
6. Check HMRC Records
7. External Calls
8. Supplying Passwords and Access to Data
9. Compile Your Own Records
10. Legal Professional Privilege
11. Excluded Material and Special Procedure Material
12. Backing Up Data
13. Restraint Orders

How to prepare and respond

1. Nominate a person to liaise with the officer in charge of the visit.

In a large office or industrial premises, it will be sensible to nominate more than one person, and the lead person might have to delegate tasks to others. Make sure that these roles are attributed to named individuals in advance as part of the policy. This is obviously not an issue if the premises is a residence or small office where only a few people work, although it would still be sensible to nominate someone so that the officer in charge knows exactly who to liaise with.

The nominated person should make him or herself known to the officer in charge and should supply the officer with the 'Search and Seizure: Information for officers' form. They should ask the officer to read the document and sign to acknowledge receipt. Provide the officer with a copy and retain a signed version at the premises. If the officer refuses to sign, note the refusal on the form and ask a colleague (if available) to sign as a witness to the refusal.

The nominated person will then take the steps outlined below or may delegate some tasks to a colleague, also identifying that colleague to the officer in charge.

At the end of the search, the nominated person(s) should gather any notes made, documents handed over or copy documents produced in the course of the visit and produce a bundle entitled 'Legally Privileged Documents'. The bundle can then be the subject of instructions to the solicitor for advice on the lawfulness of the warrants and the execution of the warrants.

2. Ask Officers to Produce Their Identification

This is important as the warrant will specify who may enter the premises. The warrant may refer to officers of HMRC, police, trading standards, a locksmith, computer expert etc. It very much depends upon what the officers expect to encounter and what they are looking for. Admissibility problems sometimes arise when a prosecutor attempts to introduce evidence seized by someone who was not entitled to be on the premises in the first place.

The officer in charge of the search might arrive with a pre-completed list of names. You should check that list against the identification provided by each officer. If an officer cannot provide identification, he/she should be asked to remain outside so that the officer in charge can be notified.

You should not physically stop officers from entering, even where you have requested that they remain outside pending identification. You should note their actions because their refusal might be challenged at a later date.

3. Notify Your Solicitor

You may ask the officers to wait for the arrival of your solicitor (particularly if you have a reasonable estimated time of arrival) or to speak with them by telephone. Not waiting for a reasonable period may result in evidential difficulties later in the case, especially if it turns out that the warrants were unlawful. Nonetheless, this is not something that the officers are bound to do and many are reluctant to wait, given that the gathering of some evidence is time critical. If they do not wait or they do not wait for a reasonable period, the timings and comments made should be noted.

The officers should (and normally do) agree to speak with your solicitor by telephone at the start of the visit. If they refuse, it should be noted and witnessed by a colleague if possible.

Your solicitor will ask questions relating to the lawfulness of the visit, the purpose and the documents/data sought. He/she will need to speak with the nominated person and may direct that person to undertake tasks.

4. The Warrant

The warrant should be presented at the time of arrival. If it is not, then you should ask to see it. As soon as you have a copy, send it directly to your solicitor for review. The warrant should specify details such as:

- the address of the premises being searched
- the categories of material they are permitted to seize
- the names of the business relevant to the investigation
- what they are not permitted to seize

It will be difficult to assess the lawfulness of the warrant in the midst of a visit when many things are happening at once. A solicitor should be able to give a preliminary opinion after considering a copy of the warrant and upon speaking with the officer in charge of the search.

Bear in mind that officers may arrive with more than one warrant, especially if they want to search vehicles or adjacent buildings. Be wary if officers say that they can use one warrant to search multiple locations. This is not normally possible.

5. Shadow and Record

In the event that your solicitor is not present, the nominated individual (and colleagues if necessary in a large operation) should shadow the HMRC officers. A note should be taken of all documents to be removed. It might not be possible to note every single document.

Recording the title of a document or label on a file may be sufficient. The most convenient way in which to note the removal of a file or document is to take a photograph of it on a mobile phone. A free scanner application on a smart phone or similar can be very effective. You should ask for copies of

important documents and you should document any refusal.

Ensure that someone has access to a phone or camera so that they can record the serial numbers of any PCs, laptops, and servers etc. to be removed from the premises. Be mindful that the phone or camera used to record information might be liable to seizure. If so, it may only be possible to use pen and paper to create the record.

If your solicitor is present, he/she will assume the role of nominated person, but may ask others to assist in providing information.

6. Check HMRC Records

HMRC should keep a record of all documents, data and hardware removed from the premises. Ensure that the description of these items is both accurate and detailed. For example, the term 'bag of papers' is not a satisfactory record of what was removed and inaccurate descriptions can cause difficulties for officers when disclosure applications are subsequently made.

You should ask to review the property registers to ensure that documents and other items are properly described and they were actually seized from the location noted on the register, e.g. 'Office at the back; on top of blue cabinet'.

7. External Calls

The accompanying document 'Search and Seizure: Information for officers' contains a notice that staff and officers are obliged to inform their line manager in the event of a visit. Ideally, this will be done before officers enter the building because the warrant(s) may include authority to seize mobile phones and other telephones and there is no guarantee that officers will act reasonably in permitting a call before a phone is seized or disabled.

The information required by line managers will differ between companies and premises. However, you will wish to confirm the time of the search, the identity of staff on the premises at the time and the approximate number of officers arriving at the premises (which gives an indication of how extensive the search might be). This will allow the company to mitigate business risk and, if the facility is available, arrange for the back-up of data which might be seized by officers in a forensic enquiry.

A serious criminal offence of prejudicing an investigation might be committed where, for example:

- officers are kept waiting outside while staff shred incriminating documents
- a member of staff discloses information to someone at another location when the disclosure is likely to prejudice the investigation

The definition of prejudice is quite broad although a defence is available if the person making the disclosure does not know or reasonably suspect that the disclosure is likely to prejudice the investigation. It is therefore important to ensure that information supplied to the line manager at

another location is designed to mitigate potential loss or business disruption without prejudicing the investigation.

Data Controllers (particularly those at another location with limited opportunity to participate in the search) will be mindful of their obligations under the Data Protection Act and potential breaches of confidentiality where seizure of computer data generally might include disclosure of sensitive information relating to a third party. This is most relevant where the third party has nothing to do with the enquiry, but their electronic data is likely to be gathered by officers who might not be aware that collection is outside the scope of the warrant or jurisdiction. In those circumstances, the Data Controller will need to decide whether or not to lock down remote access and revoke permissions upon receiving notice of a raid at relevant premises.

Any decision to block access in this way would have to be on the basis that the data is not deleted or changed in a material way pending receipt of the almost inevitable application for disclosure. Specialist legal advice is recommended where a risk of this type arises.

8. Supplying Passwords and Access to Data

When officers and computer forensic teams identify hardware they want to seize, they will not normally ask the user of that device to turn it on before it is seized. If the device is on when it is secured, a member of the forensic team will normally deal with the device to maintain its forensic integrity.

You may be asked to provide the password for a device. Refusing to do so risks arrest if the officer reasonably suspects the commission of a relevant criminal offence. Following the search and seizure exercise, the investigating authority may also issue an application requiring the subject to provide the password or un-encrypt encrypted data. A failure to do so can amount to an offence punishable with imprisonment. Simply stating that you have forgotten the password may be implausible, especially if your recent use of the device is obvious.

A refusal does not always result in arrest, and a forensic expert can often obtain a password without assistance from the user of the device. However, a refusal can raise suspicions and can prolong the investigation of the device. It is recommended that when a person is asked to disclose a password to a local device such as a mobile phone or standalone PC/laptop, the person should inform the officer that they wish to obtain legal advice before disclosing the information. This may result in the provision of passwords after the event in correspondence. This may not prevent the seizure of the item itself, but it preserves legal rights, confidentiality and data protection obligations pending legal advice.

In organisations where a network is managed remotely and employees obtain access through client software from multiple locations, central data managers may wish to consider locking-down access upon receiving notice that a raid is in progress (see above). They might do this because of their obligations under the Data Protection Act and the perceived need to verify the lawful nature of the search and seizure exercise. This risks an allegation of prejudicing an investigation and needs to be handled with great care.

Data managers also have to be mindful that if networks are locked down and are subsequently accessed voluntarily or through disclosure orders, the vast majority of attempts to hide or erase data during the lockdown period can be forensically detected. Any protocols involving the denial of access to network data during a search and seizure exercise need to be the subject of specialist legal advice, not least because the consequences of contravening the law in this respect includes a custodial sentence.

If a raid is at premises occupied by a remote user, they should notify their line manager, and if the data controller decides to revoke passwords to the network for the reasons outlined above, the remote user will simply not be able to provide the officers with a valid password. It will then be for the officers to liaise with the company and apply for disclosure.

In reality, visiting officers may not even be aware of how employees access data and will not spend time in front of a screen trying to understand what is relevant. Remember that they are not permitted to interview or interrogate subjects in the execution of the warrants. They are there to seize specified items, data and documents. If they wish to interview anyone present, they are entitled to enquire about the subject's identity for that purpose and they may be interviewed following arrest or by way of a 'voluntary interview' arranged for a date following the search.

It is important to seek expert legal advice as soon as possible because an arrest must be justified and it is sometimes possible to persuade officers that a suspect should not be arrested at the scene to facilitate an interview.

9. Compile Your Own Records

Following the raid, ensure that the nominated person compiles a detailed record of what was searched, what was removed and notes of comments made or actions taken by the officers. This might include any attempt to question or interrogate persons as suspects or any attempt to detain those present (when the questioning or detention is not in accordance with the Police and Criminal Evidence Act codes of practice). Specific legal advice on the point should be sought in the course of the raid and telephone advice is usually sufficient to resolve the matter.

The officers should provide the nominated person with a copy of the property register sheets (usually carbon copies). All of the documents should be placed in the Legally Privileged Material folder mentioned at point one above.

10. Legal Professional Privilege

Not all documents protected from examination by this status are immediately obvious, so it is good practice to ensure that relevant employees and company officers have an idea of what may be protected. Two situations can grant a document LPP status. These include:

- ***Legal advice privilege***
  These are documents containing evidence of communications between lawyer and client, where the communication amounts to 'advice'

- ***Litigation privilege***
  These are documents created for the primary purpose of obtaining legal advice or in preparation for imminent legal proceedings

In reality, officers will not normally consider the documents in any detail if there is a reasonable chance that the material might be protected by LPP. They will isolate the material for further independent consideration if it is not possible to resolve the matter one way or the other at the scene.

Some LPP material might be seized and removed in the body of the other material. It is important to notify officers as soon as this becomes apparent so that the process of examination may be suspended pending isolation of the potential LPP material.

11. Excluded Material and Special Procedure Material

On the face of the warrant, officers are not permitted to seize material classified as excluded or special procedure material. If they happen to seize it accidently, they are not permitted to examine it without an order permitting retention and examination of the material. The potential existence of material falling within this classification depends upon the nature of the business. In most cases, it will take the form of personal records and information held in confidence where the information concerns the subject's personal, spiritual or mental health. It can also include journalistic material.

If you suspect that the business involves the management of excluded or special procedure material, _ should be sought in advance so that the material can be quickly isolated and identified to the officers in the event of a visit.

12. Backing Up Data

You should always ensure that data is regularly backed up. The process of copying and returning data and servers/PCs etc. can take months. Back-ups should be kept off-site or on a cloud based facility because officers will not simply seize one copy and ignore a back-up on the same premises. They will seize both.

13. Restraint Orders

Law enforcement agencies sometimes enter premises with a warrant accompanied by a restraint order prohibiting specified individuals from dealing with their assets. Explaining the full implications of a restraint order is beyond the scope of this note, but it is important to recognise the document and seek immediate legal advice if a restraint order is served.

A failure to comply with a disclosure notice within a restraint order can amount to a contempt of court punishable by imprisonment, as can a breach of the terms of the order. They are not easily understood and a copy should be forwarded to your solicitor along with other documents mentioned above at the earliest opportunity.

For more information, contact JMW

0345 872 6666

www.jmw.co.uk