



# The Proceeds of Crime Act 2002

Practical issues and advice

## Executive summary

The Proceeds of Crime Act 2002 (POCA), which came into force in February 2003, increases the likelihood of firms having to make a disclosure. But when doing so, they may be caught between their obligation not to divulge details of the disclosure to their client, and their contractual obligations to the client. This briefing looks at the practical issues POCA raises regarding those obligations and offers some practical advice if a disclosure is necessary.

When the Proceeds of Crime Act 2002 (POCA) came into force in February 2003 it expanded, reformed and consolidated the previous multitude of money laundering offences in the UK (with the exception of those offences contained in the Terrorism Act 2000). By adding an objective test to the question of suspicion, POCA makes it more likely than under the previous regime that a firm will have to make a disclosure.

In doing so, firms may find themselves caught in the conflict between their statutory obligation not to divulge details of the disclosure to their client, and their contractual obligations to their clients. Below we look at the practical issues POCA raises about those competing obligations and offer some practical suggestions for negotiating a path through the minefield if a disclosure is necessary.

## The disclosure regime

POCA imposes on those persons working in the regulated sector the obligation to disclose any knowledge or suspicion of money laundering. An offence will be committed if the following conditions apply:

- the person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering;
- the information or other matter on which that person's knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to that person in the course of a business in the regulated sector; and

- the person fails to make the required disclosure as soon as is practicable after the information or other matter comes to him.

In addition, the new regime creates a separate offence of failing to disclose, which applies only to money laundering reporting officers (MLROs).

One notable change to the new regime is that, as well as having to satisfy themselves – based on their own knowledge or suspicion – that a person is not engaged in money laundering (the subjective test), businesses in the regulated sector and those employed by them will now also have to test that knowledge or suspicion against an objective measure. They must assess whether they have 'reasonable grounds for suspicion'. In other words, if suspicions are not aroused, should they be?

What amounts to suspicion or constitutes reasonable grounds to suspect a person is engaged in money laundering? Guidance notes issued by the Joint Money Laundering Steering Group (JMLSG) in February 2003 recognise that suspicion is subjective. The notes suggest that suspicion falls far short of proof based on firm evidence and also state that the courts have characterised suspicion as being something that is beyond mere speculation and has some foundation, albeit a lesser factual basis than would be required to form a belief.

To satisfy the test of 'reasonable grounds for suspicion' and avoid committing an offence under POCA, it is suggested that staff in the regulated sector will need to demonstrate that they took all reasonable steps in the

particular circumstances to know their customer and the rationale for a particular transaction or instruction where money laundering is alleged.

A number of practical points come out of this. The MLRO's role is to act as a filter and to assess whether concerns that employees raised with him should be disclosed to the National Criminal Intelligence Service (NCIS). To be able to make that assessment the MLRO and all employees must be fully conversant with 'Know Your Customer' procedures, insofar as they impact on their particular areas of work. For example, it seems clear that generalities or stereotypical images of certain groups or categories of people as being more likely to be involved in criminal activity will not, without more specific details pertinent to the individual customer, amount to reasonable grounds. Press coverage of recent VAT fraud raids by HM Customs & Excise has referred to the trade in mobile phones as being particularly prone to VAT evasion scams. However, the mere fact that a customer may trade in mobile phones should not itself constitute reasonable grounds to suspect, and further factors specific to that individual customer should be identified before the objective element of the test can be satisfied.

Any decision by the MLRO on whether to make a disclosure must stand up to scrutiny. More than ever, it will be important to document any decision taken and the relevant factors influencing it.

## Timing the disclosure

Once it is clear that a disclosure must be made, the next question is when to make it. Section 331(4) requires an MLRO to make a disclosure 'as soon as is practicable after the information or other matter comes to him'. As a general rule, this will mean making the disclosure before any action is taken in relation to a client's account, but the decision is not an automatic one. In this context, the firm should consider how disclosing its suspicions might affect its freedom to deal with the client's account.

The broad consequences of going ahead with a client's instruction where suspicions are aroused are clear: section 328 (which deals with 'arrangements') makes it an offence for a person to act on a client's instruction if to do so would 'facilitate the acquisition, retention, use or

control' of funds that might be the proceeds of crime, unless that person has the appropriate consent from NCIS, the police or Customs & Excise.

Consent cannot be obtained without first making a disclosure, but the legislation grants the authorities a seven-day window of investigation. Once that period has elapsed, consent is deemed to have been given (unless it is expressly refused), and the transaction may proceed. However, until the firm either has consent or the seven-day period has elapsed, the client's instruction cannot be carried out without committing a criminal offence.

The obligation to wait seven business days before conducting a transaction can have serious consequences. As a matter of commercial practice, waiting seven business days may simply not be workable. The JMLSG has recognised this, and has noted in its current guidance notes (which we understand will be updated once the Money Laundering Regulations 2003 have been published) that in some cases it may be appropriate to carry out the client's instruction, and to make the disclosure to NCIS immediately afterwards. The guidance notes suggest that the disclosure might be made after the event where:

- a transaction is already within an automated clearing or settlement system;
- the delay would give rise to a breach of contractual obligation; or
- it would breach market settlement or clearing rules.

However, the guidance notes are at pains to emphasise that disclosure after the event in the circumstances mentioned should not be automatic, and that there would need to be a reasonable excuse for not seeking prior consent.

Where it is not practicable, or where it is otherwise inappropriate to make a disclosure after the event, and where prior consent must be sought, an organisation can easily find itself caught between the competing obligations imposed by POCA and its contractual and fiduciary obligations to its customer. This conflict is brought most clearly into focus with the offence of 'tipping off'.

## Tipping off

The offence of tipping off, as set out in section 333, is committed if, knowing that a disclosure has been made to NCIS under POCA, a person 'makes a disclosure which is likely to prejudice an investigation'. In practice, this appears to mean making any kind of communication to a client which would make them aware that concerns about money laundering have been raised with NCIS.

However, this presents a firm with a major problem if it requires the consent of NCIS or another authority to conduct a transaction, but has yet to receive that consent. As noted above, in such circumstances the firm would find itself unable to carry out the proposed transaction either until consent had been specifically given, or the seven-day period had passed. In the meantime it would have no means of explaining to its client the reason why.

This predicament also raises the further prospect that even by maintaining silence as to why it had not completed a transaction, a firm could 'constructively' tip off its client: the firm is obliged to act in such an uncharacteristic way that it leads the client to infer that a disclosure must have been made about its activities. Customs & Excise have accepted that this consequence of operating the tipping off provisions is undesirable, but believe it represents a less offensive course of conduct than positively divulging details of the disclosure to a client.

### So what can a firm tell its client?

Case law relating to offences under the old money laundering regime provides some guidance, which, from our experience, it seems that investigating authorities are keen to adhere to. The key issue in the offence of tipping off is whether a communication to the client will prejudice any ongoing investigation. Whether that will be the case can be best judged by the investigating authorities themselves. It is important to establish good communications with the relevant authority at an early stage, and to discuss with them what may be disclosed without 'tipping off' the client. This approach has been supported by the court in the first instance decision in *P v P* [2003] EWHC 2260 (fam) (Times Law Report 14 October 2003).

Our recent experience of working alongside Customs & Excise suggests that they viewed positively the approach of engaging them in the process from the outset. Clearly the purpose of such a dialogue is to reach a consensus on what may be disclosed to a client. If it is not possible to reach a consensus, the next stage is to seek a declaration from the court on what may be disclosed.

To the extent that the investigating authority considers that an investigation may be prejudiced, it will be for that authority to satisfy the court that its view is reasonable. A paper trail of correspondence with the investigating authority will help the court to reach a decision. Investigating authorities recognise the situation in which institutions can innocently find themselves and in our experience they are willing to assist constructively.

It is important to be aware that the risk of tipping off may continue beyond the end of a specific transaction. The potential for prejudicing an ongoing investigation will continue for as long as the investigation itself lasts, which may be a considerable time. It is essential that the institution maintains tight control over the dissemination of information relating to any disclosure made to NCIS.

As a general rule, given the large number of possible points of contact between the different departments of a firm and its client, the MLRO and his or her immediate team should, in practice, only divulge details of the disclosure within the organisation's network on a 'need to know' basis. This means that where details of the disclosure are passed on internally within an organisation, it must be made plain to the recipient that he or she should exercise extreme caution in disseminating the information further, and that the potential for criminal sanction hangs over the head of anyone passing on that information if an investigation is prejudiced as a result.

A wider concern is the effect of a disclosure on a firm's ongoing relationship with its client (with the possibility that the firm may have to disregard a client instruction in the absence of consent). In the worst scenario, a refusal to carry out a client's instruction, because to do so would be to commit a criminal offence, may cause the client loss and potentially result in litigation. Clearly this is undesirable, particularly where the circumstances causing the dispute are not of the firm's own making.

How, then, to guard against this litigation risk? When similar situations were brought before the courts under the old regime, such as in the Court of Appeal case of *C v S and others* [1999] 2 All ER 242, the court expressed sympathy with the firm but did not go far in offering guidance on how the problem might be avoided in the future.

The new regime has been put to the test in the courts in *P v P*. In this case, the judge decided that where the appropriate consent was refused and a 31-day moratorium imposed, the firm and NCIS or other relevant body should try to agree on the degree of information that could be disclosed during that moratorium period without harming the investigation. The prohibition on disclosing information that may prejudice an investigation does not mean that a firm cannot disclose any information at all to its client. *P v P* has reinforced the recommendation in *C v S* that in such situations, the firm should try to agree with the authorities what information can be disclosed without prejudicing the investigation. Should they be unreasonably difficult about agreeing, it would be open to the firm to apply to the court and obtain an explanation from the authorities as to why they were refusing to agree to the terms and extent of the disclosure.

One area in which firms can lessen their potential exposure is in the terms of business governing the operation of client accounts. Typically, these will contain exclusions of liability covering situations where statutory and contractual obligations conflict. In the new world of POCA, financial institutions should consider whether the existing exclusions in their terms and conditions cater sufficiently for the impact of money laundering legislation.

## Conclusion

The new regime under POCA potentially sets a number of traps for the unwary. As a result, firms will need to operate with care, and will need to ensure they can demonstrate that they have acted reasonably in responding to the requirements of POCA. Provided they act honestly and consistently, however, and monitor client relationships with care, it is less likely that they will be criminally prosecuted.

For further information please contact	Tim Cave
	T + 44 20 7832 7313
	F + 44 20 7832 7001
	E <a href="mailto:tim.cave@freshfields.com">tim.cave@freshfields.com</a>
	David Scott
	T + 44 20 7832 7379
	F + 44 20 7832 7001
	E <a href="mailto:david.scott@freshfields.com">david.scott@freshfields.com</a>