THE UK'S ANTI-MONEY LAUNDERING LEGISLATION AND THE DATA PROTECTION ACT 1998

GUIDANCE NOTES FOR THE FINANCIAL SECTOR

April 2002

Introduction

1. This guidance has been prepared by the Government departments that co-ordinate the UK's anti-money laundering legislation in response to concerns expressed by some banks and other financial institutions about the interaction between anti-money laundering laws and the Data Protection Act 1998 (DPA). It has been discussed with the Information Commissioner, who supports the approach taken.

2. In particular, this guidance addresses the relationship between the obligation not to 'tip off' an individual about whom a Suspicious Transaction Report (STR) has been made on the one hand, and the individual's right of access to his personal data and the corresponding obligations on financial institutions on the other.

3. Please note that this guidance has no legal status. If you are concerned about any aspect of compliance with money laundering legislation or the DPA you should seek independent legal advice.

The UK's anti-money laundering legislation

4. The UK has fulfilled its international obligations to create money laundering offences in several pieces of primary legislation – the Criminal Justice Act 1988 (as amended), the Drug Trafficking Act 1994 and the Terrorism Act 2000 (as amended). These create two different types of obligation to make STRs. In both cases, an STR can be made either to the law enforcement authorities or, where the individual works for an employer who has a Money Laundering Reporting Officer (MLRO), to the MLRO. Once a report is made to an MLRO the responsibility rests on him to decide whether to make a report to the law enforcement authorities.

5. The first obligation to make STRs is that each of the statutes listed above requires that a person must make an STR if he knows or suspects that **he or his organisation** is about to become involved in money laundering. For example, a solicitor who suspects that he is being asked to put funds into his client account in order to conceal their criminal origin would be obliged to make an STR and obtain the consent of the authorities before carrying out the transaction. If he

does not make the STR and gain the consent, he will be guilty of a money laundering offence if he puts the funds into his client account. The solicitor can make the STR after putting the funds into his client account if he has a good reason for not making it before.

6. The second obligation to make STRs is that the Drug Trafficking Act and the Terrorism Act contain offences of "failure to report". These are committed where a person knows or suspects (or, in the case of the Terrorism Act, has reasonable grounds for knowing or suspecting) that **another person** is engaged in laundering either the proceeds of drug trafficking or terrorism related property but does not make a report to the law enforcement authorities.

7. The Money Laundering Regulations 1993 oblige financial institutions to ensure that they have systems in place to make STRs to the National Criminal Intelligence Service (NCIS).

8. The Proceeds of Crime Bill will consolidate the provisions of the Drug Trafficking Act and the Criminal Justice Act so that the law on laundering the proceeds of drug trafficking and laundering the proceeds of other crime is contained in one piece of legislation. The obligation on people who become personally involved in money laundering to make STRs will not change significantly. However, the Bill extends the Drug Trafficking Act offence of failure to report another's involvement in money laundering in two respects. First, the provision is brought in line with the Terrorism Act so that a person must make an STR if he has 'reasonable grounds to believe' that another person is engaged in money laundering. Second, the obligation to make an STR will no longer be restricted to the situation where another person is laundering the proceeds of drug trafficking, but will be extended to the laundering of the proceeds of **any crime**. In order to take account of these extensions, the failure to report offence is now limited to people who come across the information about money laundering in the course of conducting business in the "regulated sector". "Regulated sector" is defined in Schedule 6 to the Bill. Broadly, it currently encompasses every institution that is obliged to comply with the Money Laundering Regulations.

9. The Proceeds of Crime Bill will replace the money laundering provisions in the Criminal Justice Act and the Drug Trafficking Act. However, the Terrorism Act will continue to regulate the laundering of funds for terrorist purposes.

'Tipping Off'

10. In order to prevent individuals from warning those about whom they have made an STR, the money laundering legislation also criminalises 'tipping off'. Where a person knows or suspects that an STR has been made to the law enforcement authorities, it is an offence for him to

make any disclosure which is likely to prejudice any investigation which might be conducted following the making of the STR. The most obvious example of a disclosure likely to prejudice an investigation is letting an individual know that the authorities are interested in him so that he has time to destroy evidence.

11. No offence is committed where disclosure of an STR would not be likely to prejudice an investigation. For example, where the existence and contents of an STR have been revealed in the course of criminal proceedings, it is unlikely that any prejudice would be caused by the subsequent disclosure of the STR to the individual concerned. Similarly, in the case of an STR made many years ago and in relation to which the file has long since closed, it seems unlikely that any prejudice would be caused by disclosing the STR.

12. In cases where financial institutions are concerned about how to avoid arousing suspicion in a customer that one of their transactions is being investigated, they should contact NCIS for advice on how to deal with that customer.

The Data Protection Act

13. Under section 7 of the DPA, on making a request in writing to a data controller (i.e. any organisation which holds personal data), an individual is entitled:

- to be informed whether the data controller is processing (which includes merely holding) his personal data; and if so
- to be given a description of those data, the purposes for which they are being processed and to whom they are or may be disclosed; and
- to have communicated to him in an intelligible form all the information which constitutes his personal data and any information available to the data controller as to the source of those data.

14. Such a request is known as a Subject Access Request. Data controllers must respond to subject access requests promptly, and in any case within 40 days. The 40 days begin from when the data controller has received the request, any further information he may need to identify the applicant and locate the personal data sought, and, if he charges one, the fee (of up to £10 maximum).

15. Data controllers may withhold information identifying another individual, for example information identifying a bank teller as the source of the data, unless that individual has consented to the disclosure or it is reasonable in all the circumstances to disclose the information without their consent (see sections 7(4) to 7(6) of the DPA).

16. The DPA provides certain exemptions to the right of subject access, of which section 29 is the most relevant in the present context. This provides that personal data are exempt from section 7 in any case to the extent to which the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

17. Even when relying on an exemption data controllers should provide as much information as they can in response to a Subject Access Request.

Section 7 and Tipping Off

18. Concerns have been raised as to the interrelation of the tipping off provisions and section 7 of the DPA.

19. The starting point is the similar language used in the tipping off offence (disclosure would be likely to prejudice any investigation which might be conducted following the making of the STR) and the DPA section 29 exemption (disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders). In summary, where disclosure of a particular STR would constitute a tipping off offence, the section 29 exemption will apply, and where disclosure of an STR would not constitute a tipping off offence, the section 29 exemption will not be available in respect of the money laundering element. However it must be emphasised that each request for information must be considered on its merits, as explained in more detail below.

How to deal with a Subject Access Request

20. To take an example, Mr X deposits £500,000 in cash into his bank account and immediately transfers it to an offshore account. The bank is suspicious that this may represent money laundering and so sends an STR to NCIS. NCIS pass the STR to a police force and await further information.

21. Mr X then makes a Subject Access Request to the bank under section 7 of the DPA. The bank is now caught in a seemingly difficult position – should they disclose the STR to Mr X and risk committing the tipping off offence, or should they withhold it, and risk breaching the DPA?

22. It is impossible to lay down any general rules as to how to deal with a subject access request, as the requirements of section 7 DPA and the application of section 29 DPA must be considered on a case-by-case basis. It should never be assumed that the section 29 exemption applies automatically to STRs. Each time a Subject Access Request is received, the institution concerned must carefully consider whether, *in*

that particular case, disclosure of the STR would be likely to prejudice the prevention or detection of crime.

23. In determining whether the section 29 exemption applies, it is legitimate to take account of the particular way in which financial crime is investigated. The detection of money laundering often depends on fitting together a number of separate pieces of information. Thus even though a particular piece of information (e.g. an individual STR) does not show clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of the jigsaw which enables law enforcement agencies to detect crime.

24. Where a financial institution is in doubt as to whether disclosure would be likely to prejudice an investigation or potential investigation, it should approach NCIS for guidance. Institutions should bear in mind the requirement to respond *promptly* to a Subject Access Request *and in any event* within 40 days and ensure that they approach NCIS in good time.

25. It should be noted that, where an institution withholds a piece of information in reliance on the DPA section 29 exemption, it is not obliged to tell the individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the request.

26. Data controllers may wish to keep a record of the steps they have taken in determining whether disclosure of an STR would involve 'tipping off' and\or the availability of the section 29 exemption. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner or the courts.

Internal reports

27. When a bank clerk makes an STR to his Money Laundering Reporting Officer (MLRO) but the MLRO has not passed on an STR to NCIS, the principles outlined above also apply. While this particular STR may not have raised enough suspicion for the MLRO to deem it worth passing to NCIS, the internal STR may be the basis for establishing a pattern of future transactions that arouse suspicion. Therefore when dealing with a Subject Access Request the same considerations apply as set out above.

28. If the institution considers that disclosure of an STR made by a bank clerk would be likely to prejudice the prevention or detection of crime, even if the STR has not been passed to NCIS, then section 29 may be relied on to withhold that information.

Summary

29. Section 29 does not provide a blanket exemption to subject access obligations for STRs; each request for information must be considered on its merits. Institutions must consider whether, in the particular case, disclosure of the STR would be likely to prejudice the prevention or detection of crime.

    - Where telling an individual that an STR relating to him has been made would constitute a 'tipping off' offence, that information can be withheld in reliance on section 29 of the DPA. This applies even where the STR has not been passed to NCIS.

    - Where disclosure of an STR would not constitute a 'tipping off' offence the section 29 exemption will not be available in respect of the money laundering element.

Comments

30. The Government will review this guidance within the next three years. If you have any questions or comments, please contact:

    The Financial Crime Branch,
    HM Treasury,
    Allington Towers,
    19 Allington Street,
    London,
    SW1E 5EB

NB from August 2002:

    The Financial Crime Branch,
    HM Treasury,
    1 Horse Guards Road,
    London,
    SW1A 2HQ