HOUSE OF LORDS

European Union Committee

6th Report of Session 2010–11

Money laundering: data protection for suspicious activity reports

Report

Ordered to be printed 18 January 2011 and published 20 January 2011

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£6.00

HL Paper 82

The European Union Committee

The Committee considers EU documents in advance of decisions being taken on them in Brussels, in order to influence the Government's position and to hold them to account.

The Government are required to deposit EU documents in Parliament, and to produce within two weeks an Explanatory Memorandum setting out the implications for the UK. The Committee examines these documents, and 'holds under scrutiny' any about which it has concerns, entering into correspondence with the relevant Minister until satisfied. Letters must be answered within two weeks. Under the 'scrutiny reserve resolution', the Government may not agree in the EU Council of Ministers to any proposal still held under scrutiny; reasons must be given for any breach.

The Committee also conducts inquiries and makes reports. The Government are required to respond in writing to a report's recommendations within two months of publication. If the report is for debate, then there is a debate in the House of Lords, which a Minister attends and responds to.

The Committee has seven Sub-Committees which are:
Economic and Financial Affairs and International Trade (Sub-Committee A)
Internal Market, Energy and Transport (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Agriculture, Fisheries and Environment (Sub-Committee D)
Justice and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social Policies and Consumer Protection (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Bowness
Lord Carter of Coles
Lord Dear
Lord Dykes
Lord Hannay of Chiswick
Lord Harrison
Baroness Howarth of Breckland
Lord Jopling
Lord Liddle
Lord Maclennan of Rogart
Baroness O'Cathain
Lord Plumb
Lord Richard
Lord Roper (Chairman)
The Earl of Sandwich
Lord Teverson
Lord Tomlinson
Lord Trimble
Baroness Young of Hornsey

The Members of the Sub-Committee which prepared this report are listed in Appendix 1.

Information about the Committee

For information freely available on the web, our homepage is http://www.parliament.uk/hleu
There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at http://www.parliament.uk/about_lords/about_lords.cfm

Sub-Committee Staff

The current staff of the Sub-Committee are Michael Collon (Clerk), Michael Torrance (Policy Analyst) and Joanna Lukens (Committee Assistant).

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.
General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A 0PW
General enquiries 020 7219 5791. The Committee's email address is euclords@parliament.uk

CONTENTS

Money laundering: data protection for suspicious activity reports

Introduction

1. In July 2009 we submitted to the House a report on Money laundering and the financing of terrorism.[1] On 7 December 2009 the House debated that report. In this further report we explain developments following some of the recommendations in our first report.[2]
2. The authorities of Member States rely in their fight against money laundering largely on information supplied by the private regulated sector. Banks, insurers, lawyers, accountants and many other persons and bodies who handle money on behalf of others are required to report any suspicious transactions to the authorities. Chapter III of the Third Money Laundering Directive[3] imposes on the regulated sector a duty to report to the national Financial Intelligence Unit (FIU) any transaction or activity which seems to involve funds which are the proceeds of criminal activity. These reports are suspicious activity reports, or SARs.[4]
3. The FIU for the United Kingdom is the Serious Organised Crime Agency, SOCA. The SARs are entered onto a database maintained by SOCA known as ELMER. In evidence given to our inquiry in March 2009 the Director of the FIU said that there were then about 1.5 million entries on the database.[5] The number increases by more than 200,000 each year.[6] On that basis there are likely now to be some 400,000 more SARs on the database than there were then.
4. We do not question the purpose of the SARs regime in the fight against money laundering and the financing of terrorism. Examples are given each year in the SARs Regime Annual Report published by SOCA. But the wide access to what is in effect a database of suspects led us to have serious concerns about data protection issues, which are set out in full in paragraphs 174–181 of our first report.
5. We recommended that the Information Commissioner should review and report on the operation and use of the ELMER database, and should consider in particular whether the rules for the retention of data were compatible with the jurisprudence of the European Court of Human Rights. In their response[7] the Government told us that SOCA had invited the Information Commissioner to meet its board to discuss taking this

---

1 19th Report, Session 2008–09, HL Paper 132-I and 132-II.

2 This report was prepared by the Home Affairs Sub-Committee, whose members are listed in Appendix 1. The members of the Sub-Committee who prepared our first report are listed in Appendix 1 to that report.

3 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L309 of 25 November 2005.

4 A full description of the SARs regime is given in Chapter 4 of our first report.

5 19th Report, Session 2008–09, HL Paper 132-II, Q 193.

6 There were 210,524 new SARs in the year to end September 2008; 228,834 to September 2009; and 240,582 to September 2010: SARs Regime Annual Reports for 2008 (page 40), 2009 (page 45) and 2010 (page 55).

7 Cm 7718, 6 October 2009.

recommendation forward. The Government stated that access to the database would be limited to adequately trained staff from "appropriate public bodies", an expression which did little to reassure us. We raised the issue again when the report was debated, and Lord Brett replied that the Information Commissioner was planning to implement our recommendation in the form of a review.[8]

The report of the Information Commissioner

6. On 29 November 2010 the Information Commissioner wrote to the Chairman enclosing his report to this Committee on SOCA's operation and use of the ELMER database. We are grateful to the Commissioner and his staff for his very full report, plainly the culmination of a thorough review of all the matters which troubled us.

7. On 28 July 2010 Baroness Neville-Jones, the Minister of State at the Home Office, stated in reply to a written question: "It is proposed that the [Information Commissioner's] report will be made available in the first instance to the House of Lords EU Committee that commissioned it. Arrangements for its wider publication will be considered after the Committee has had an opportunity to consider it."[9] We print the Commissioner's report as Appendix 2 to this report to give it the wider publicity which in our view it deserves and requires.

8. From our perspective, the most significant finding of the Commissioner is his conclusion (paragraph 5.7) that "there are several aspects of the operation of ELMER which raise concerns about compliance with the Data Protection Act"—concerns which the Commissioner then sets out in full. In paragraph 6.1 of his report he makes "a number of recommendations to help ensure that the processing of personal data on the ELMER database complies with the requirements of the Data Protection Act …" The first four of these recommendations are addressed to SOCA, the fifth to the Government. Accordingly on 15 December 2010 the Chairman wrote to Lord Sassoon, the Commercial Secretary to the Treasury, enclosing a copy of the Commissioner's report, and asking for his reaction to the Commissioner's recommendations. We print the text of that letter in Appendix 3. Responsibility for money laundering is divided between the Treasury and the Home Office, and the Chairman's letter was copied to Baroness Neville-Jones.

Access to the database

9. At this stage we wish to make only two comments. The first relates to access to the database. Our statement in paragraph 175 of our first report that access to ELMER is available to "agencies such as trading standards, and some county councils" is a direct quotation from the evidence which the Director of the FIU gave us on 18 March 2009.[10] Our further statement that "Nottinghamshire County Council uses ELMER to investigate housing

---

8 HL Deb 7 December 2009 col 976.

9 HL Deb 28 July 2010 col WA 362.

10 For the very full reply, reference should be made to our first report: 19th Report, Session 2008–09, HL Paper 132-II, Q 193. The relevant extract reads: "At the same time that entire database is made available to over 75 different UK agencies. When I say 'made available', it is now desk-top accessed to investigators from every police force in England and Wales, Scotland and Northern Ireland, all of the national agencies that have prosecution powers—HMRC, DWP, the Serious Fraud Office, together with other agencies such as trading standards, and some county councils."

benefit fraud" is taken from a reply to a question from Lord Marlesford given by Lord West of Spithead, then Parliamentary Under-Secretary of State at the Home Office.[11]

10. A year after the publication of our report, Baroness Neville-Jones stated that "Direct access to the Elmer database by Neath Port Talbot County Borough Council has been suspended while SOCA carries out a review of end-user access." We infer from this that Neath Port Talbot County Borough Council had direct access to the database until shortly before then.[12]

11. However in paragraph 4.14 of his report the Commissioner states: "The review team's findings suggest that access is not in fact as wide as suggested in the [Committee's] report. The review team were advised that no Local Authorities or Trading Standards bodies have direct access to ELMER as yet although agencies that have investigative and enforcement powers such as the Financial Services Authority, Trading Standards Investigation Units and local authorities' Fraud Investigation Units may request SAR derived information from SOCA. These requests are risk assessed before information is disclosed." If the only change since we reported is that local authorities no longer have direct "desk-top" access (the expression used by the Director of the FIU) or access "from a terminal in a local police unit" (Lord West's answer) but still have indirect access, again this does little to reassure us.

Proportionality of the SARs system

12. The Commissioner's last recommendation is "That the Government considers whether, in the light of experience, the current arrangements for reporting of SARs continue to be justified, whether they are both effective and proportionate and whether they could be improved. Consideration should be given to whether there is a pressing social need to justify the requirement to report any transactions which is based on [a] very low threshold of suspicion that handling criminal property or money laundering is taking place."

13. In paragraphs 101–110 of our first report we expressed our concern that the current reporting arrangements were disproportionate. In particular we criticised the "all crimes" approach, which requires an activity suspected to involve property which might be laundered to be reported no matter how trivial the underlying criminal offence. We pointed out that Recommendation 1 of the Financial Action Task Force does not require this; nor does Article 20 of the EU Directive, since money laundering is defined by reference to "criminal involvement in the commission of a serious crime".[13] We suggested a *de minimis* exclusion for the reporting of suspicious activities.

14. In their response, the Government strongly defended the "all crimes" approach, and argued that a *de minimis* exclusion would be unworkable. They

---

11 HL Deb 2 April 2009 cols 287–288. The full answer reads: "There is an accredited financial investigator in Nottingham [sic] County Council who is able to access and use the Serious Organised Crime Agency's database of Suspicious Activity Reports (SARs) from a terminal in a local police unit. The financial investigator uses SARs when investigating housing benefit fraud. No other local authority currently has access to the SARs database. Accredited financial investigators were established in the Proceeds of Crime Act 2002. The Proceeds of Crime Act 2002 (References to Financial Investigators) (Amendment) Order 2005 (SI 2005/386) added local authority fraud investigators to the list of financial investigators who could use various powers in the Act."

12 HL Deb 28 July 2010 col WA 362.

13 Articles 1(2)(a), 3(4) and 3(5).

did however undertake to work with the Law Society to review ways of re-focusing the definition of money laundering and money laundering offences.[14]

15. We hope that, when the Government consider the Commissioner's doubts about the justification of reporting transactions where there is a very low level of suspicion, they will also give further consideration to our own concerns about the requirement to report suspicions about the commission of trivial criminal offences. We recall and reiterate the recommendation in our first report[15] that **consideration should be given to amending the Proceeds of Crime Act 2002 to include a *de minimis* exclusion.**

Conclusion

16. We believe that the Information Commissioner's report justifies our view that the ELMER database is not fully compliant with the Data Protection Act and the Human Rights Act. We look forward to hearing from ministers what steps the Government and SOCA will take to comply with the Commissioner's recommendations, and ours.

17. **We make this report to the House for debate.**

---

[14] Supplementary memorandum by the Law Society of England and Wales, paragraph 2.12: 19th Report, Session 2008–09, HL Paper 132-II, page 34.

[15] Ibid, paragraph 110.

APPENDIX 1: HOME AFFAIRS SUB-COMMITTEE

The members of the Sub-Committee which prepared this report were:

Lord Avebury
Lord Dear
Baroness Eccles of Moulton
Lord Hannay of Chiswick (Chairman)
Lord Hodgson of Astley Abbotts
Lord Judd
Lord Mackenzie of Framwellgate
Lord Mawson
Lord Richard
Lord Tomlinson
Lord Tope

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:
http://www.publications.parliament.uk/pa/ld/ldreg.htm

APPENDIX 2: REPORT FROM THE INFORMATION COMMISSIONER

The Serious Organised Crime Agency's operation and use of the ELMER database.

Information Commissioner's Report to the House of Lords European Union Committee

Index

1. Introduction

1.1 The Information Commissioner (the Commissioner) has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can and taking appropriate action where the law is broken.

1.2 The House of Lords European Union Committee ('the Committee') published the findings from its Inquiry into Money Laundering and the Financing of Terrorism in July 2009. The Committee made a number of recommendations which included recommending that the Commissioner should review and report on the operation and use of the ELMER database. It also recommended that the Commissioner should consider in particular whether the rules for the retention of data are compatible with the jurisprudence of the European Court of Human Rights.

1.3 The Commissioner welcomed the opportunity to undertake the review of the ELMER database. As part of the Commissioner's review a team ('the review team') from the Commissioner's Office visited the Serious Organised Crime Agency ('SOCA') to observe the ELMER database in operation. This enabled the review team to understand the type of information that is recorded and retained on ELMER and the purposes for which it is used.

1.4 The review team received the fullest co-operation from SOCA and were able to have access to staff and to see the operation of the database in practice. The Commissioner thanks SOCA and its staff for their assistance.

2. Background

2.1 There is a legal obligation for the regulated sector and any entity (individual or corporate, regulated or unregulated) that might otherwise be accused of committing one of the principal money laundering offences under Section 327 to 329 of the Proceeds of Crime Act to submit Suspicious Activity Reports (SARs) to SOCA. The 'regulated sector' includes banks and financial institutions and more recently has included solicitors, accountants and others. It is estimated that between 125,000 and 175,000 businesses could be subject to reporting requirements although we understand that only approximately 5,000 actually report. The ELMER database holds the SARs information and currently holds approximately 1.5 million SARs.

2.2 A SAR must be made as soon as practicable once an organisation (or an individual) has formed a suspicion or knows of terrorist financing or money laundering. It is a criminal offence not to make a disclosure when a suspicion has been formed although the legislation does not define 'suspicion' and this has been left to the Courts. In the Court of Appeal case R v Da Silva [2006] All ER (D) 131 (Jul) the Judge stated that there should be 'more than a fanciful possibility' that a person is handling criminal property or money-laundering activity is taking place. Guidance issued by SOCA states 'As soon as you know or suspect that a person is engaged in money laundering or dealing in criminal property you must submit a SAR'. SOCA also provides a document containing case studies for training purposes and highlights those situations where a SAR may be required such as where there is sudden activity on a dormant account.

2.3 The SARs regime was introduced in 1986/87. However ELMER only became functional in 2000. SARs submitted prior to ELMER becoming functional were transferred to the ELMER database. This means that as at 2010 data has been held on ELMER for ten years but is actually older in some cases.

2.4 Latest figures indicate that from October 2008 to the end of September 2009 228,834 SARs and 13,618 Consent SARs were received by SOCA[16]. In 2009 an average of 19,264 were being received monthly.

2.5 During the Committee's Inquiry the Commissioner stressed that it was important that the SAR process should be operated in a proportionate manner. The database should focus on assisting with the investigation and prevention of serious criminal behaviour and the thresholds for reporting, recording and granting access should reflect this. It should be noted that the rationale for the ELMER database and the range, content and reason for submission stem from the reporting provisions in the Proceeds of Crime Act 2002 and the Terrorism Act 2000 rather than a requirement of SOCA.

2.6 It was also the Commissioner's view that there should be established retention periods for the information held on the database. If there are SARs based on financial transactions meeting a particular threshold level rather than on hard evidence of criminal activity the prolonged retention of those records would be inappropriate and disproportionate and there should not be a blanket policy to keep all SARs indefinitely. SOCA clarified in evidence that each SAR is assigned a deletion date of ten years after receipt and is automatically deleted unless it has been amended or updated in which case the deletion date is reset to six years following that event. SOCA also confirmed that there is also a procedure for earlier deletion of individual SARs where all necessary activity relating to that SAR has been undertaken and SOCA estimated that 20,880 SARs have been permanently deleted from the database.

2.7 The Committee were concerned that SARs are routinely retained for ten years on a database to which there is wide access especially in those cases where it could be shown that the initial suspicion was unfounded. The Committee referred particularly to the ruling of the European Court of Human Rights that the retention on the DNA database of the DNA of persons not convicted of a criminal offence could amount to a breach of their right to respect for private life under Article 8 of the European Convention on Human Rights.[17]

2.8 The Committee hoped that adoption of their recommendations on a de minimis provision, improved guidance and the improved provision of feedback to

---

16 SOCA Annual Report 2009

17 S and Marper v United Kingdom, judgment of 4 December 2008, http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843941&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

reporters would lead over time to an improvement in the quality of the ELMER database so that entries on it are focused on serious organised crime including money laundering. The Committee's recommendation in this respect was in relation to removing the requirement to report a suspicious transaction based on a minor offence. This would lead to the raising of the threshold for making SARs leading to a more proportionate approach.

3. Legal framework

3.1 There is an established legal framework governing the requirements to notify SOCA of a SAR. These have grown over time and relate to a number of legal instruments (see Annex 2).

3.2 The legislation which directly relates to the way in which the ELMER database operates are the Proceeds of Crime Act 2002 and the Terrorism Act 2000 which require banks and other businesses in the 'regulated sector' together with any entity (individual or corporate, regulated or unregulated) that might otherwise be accused of committing one of the principal money laundering offences ('the principal money laundering offences') to report. These offences are outlined in Sections 327 to 329 of the Proceeds of Crime Act and include concealing criminal property, disguising criminal property, converting criminal property, transferring criminal property and removing criminal property from England and Wales.

3.3 These organisations/individuals are required to report to the UK Financial Intelligence Unit (SOCA) any suspicions that arise concerning criminal property, money laundering or terrorist financing. Persons and businesses can avail themselves of a defence against money laundering charges by seeking the consent of SOCA to proceed with a transaction or undertake an activity (a prohibited act) about which they have concerns. The decision to grant or refuse consent is taken by SOCA after consultation with other Law Enforcement Agencies (LEAs).

The Data Protection Act 1998

3.4 The DPA establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

3.5 Central to the DPA are eight legally enforceable principles which include that organisations must ensure that everything they do with personal information is fair and lawful, and that the information is used only for specified purposes. Personal information must also be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. Personal information should not be kept for longer than is necessary and appropriate technical and organisational measures need to be taken against unauthorised or unlawful processing or loss.

3.6 The Commissioner is responsible for enforcing the DPA and has enforcement powers to ensure compliance.

The Human Rights Act 1998

3.7 The Human Rights Act 1998 (HRA) gives legal effect in the UK to the fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR). SOCA is a public authority for the purposes of the HRA.

3.8 Article 8 of the ECHR gives every person the right to "respect for his private and family life, his home and his correspondence." Article 8(2) states that there "shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

S and Marper v UK

3.9 In S and Marper v The United Kingdom (Application Nos 30562/04 and 30566/04, 2008) the European Court of Human Rights (ECtHR) found that "the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the …applicants, fail[ed] to strike a fair balance between the competing public and private interests…". The Court established that the retention constituted "a disproportionate interference with the applicants' right to respect for private life and [could not] be regarded as necessary in a democratic society". Accordingly, it found the UK to be acting in violation of Article 8 of the European Convention of Human Rights (ECHR).

4. Findings

4.1 There is no single prescribed way to submit SARs. They can be submitted several ways such as online using SOCA SAR Online via the SOCA website, by fax, by post or telephone. SAR Online allows SARs to be submitted securely. SAR Online is for small to medium volume reporters who register, log on and then submit their reports. High volume reporters such as banks make multiple submissions of SARs via an encrypted email process which allows for secure bulk data exchange. SARs received electronically receive an automatic Unique Reference Number and confirmation of receipt. However, approximately 3% of reports are received by fax or post and these SARs do not receive an acknowledgement of receipt unless the reporter requests consent to carry out a transaction.

4.2 In order to submit a SAR via SAR Online a new user is required to register and, to do this, they must enter the details of the reporting organisation they represent. The user will then need to activate the account before it can be used and then will be prompted to create a password. Once that is created the user will be able to utilise the site functionality which is essentially completing the form and submitting it. Registered users can also nominate other users.

4.3 SOCA guidance states that the following information should be contained in a SAR if available to the reporter—subject's full name, date of birth and addresses, subject details such as national insurance numbers, vehicle registration, driving licence, passport, phone numbers, website addresses, details of occupation/employer, details of any associates of the subject, company details including full legal name, designation, country of incorporation and contact details, subject's account number if appropriate and transaction details and subject type such as subject, victim etc. A full reason for any suspicion should also be provided.

4.4 Bulk transfers (via SAR Online) can include 300 to 400 SARs in one email (which is encrypted). The review team were advised that ELMER would be unlikely to include duplicates as this would only happen if the organisation submitted the information twice.

4.5 SARs which are received via SAR Online are automatically added to the ELMER database. An automatic keyword search identifies those SARs which may require further investigation. Manual searches can also be undertaken on the database as and when required.

Consent SARs

4.6 The Proceeds of Crime Act requires that the regulated sector and any entity (individual or corporate, regulated or unregulated) that might otherwise be

accused of committing one of the principal money laundering offences not only report but also seek consent from the designated authority (SOCA) to carry out a transaction. This would be when there is a suspicion that they may be dealing with the proceeds of crime and that to complete the transaction could mean that a money laundering offence is committed.

4.7 Individuals and organisations can therefore avail themselves of a defence against money laundering charges by seeking the consent of SOCA to conduct a transaction or undertake an activity about which they have concerns. The legislation gives SOCA seven working days to respond. Although a transaction must not be carried out until specific consent is received, in practice the assumption is that if the reporter (or consent requestor) has not heard back from SOCA within seven days consent can be assumed.

4.8 If consent is refused the transaction or activity must not proceed for a further 31 calendar days ('moratorium' period) with the intention that action will be taken by investigators within that time. If consent is granted following the moratorium period the transaction can progress and the reporter will have a defence to any potential money laundering offences. Also, the reporter will have a defence if the moratorium period expires and no action has been taken and the reporter proceeds with the transaction. SOCA advised that approximately 13,000 consent SARs are received annually.

Access

4.9 Access to ELMER by external agencies is through the Moneyweb portal. The review team were shown how this works in practice. Most records are accessible through the Moneyweb portal although those which are considered to be particularly sensitive are not available to view (such as terrorist financing and those involving corrupt officials). Records only become accessible after they have been on ELMER for seven days.

4.10 Currently 2,200 individual users have access via Moneyweb. This is monitored and where, for example, an account is not being used this would be reviewed. A Security Certificate is issued when a user registers and this is renewed annually. The Security Certificate is attached to the unique email address which is registered to the account and therefore users are not able to log in from their home address or indeed another organisation or police force if they re-locate or change jobs. In these cases they would need to re-register.

4.11 All organisations registering to use Moneyweb sign a Partnership Agreement. This stipulates who will be eligible to access the system, the type of training required, SOCA's responsibilities and the responsibilities of the end user including confidentiality. Partnership Agreements are signed at senior level.

4.12 Each organisation registering will have a SPOC (Single Point of Contact) for the purposes of this work and they report on the use of the system. SOCA also undertakes visits and is in regular contact with the SPOCs. SOCA provides six monthly feedback to users by way of the Feedback Questionnaire and also monitors the activity of new users. SARs were reviewed by end users through Moneyweb 362,229 times during the period January to October 2010.

4.13 The Committee's report states that access to ELMER is available to 'every police force in England and Wales, Scotland, Northern Ireland, all of the national agencies that have prosecution powers—HMRC, DWP, the Serious Fraud Office—together with other agencies such as trading standards, and some county councils … every day there are over 1,500 trained and authorised users across the country who as their core business are examining SARs that relate to their own public duty. It is also used for purposes unrelated to serious organised crime, such

as ensuring compliance with tax obligations. Nottinghamshire County Council uses ELMER to investigate housing benefit fraud.'

4.14 The review team's findings suggest that access is not in fact as wide as suggested in the report. The review team were advised that no Local Authorities or Trading Standards bodies have direct access to ELMER as yet although agencies that have investigative and enforcement powers such as the Financial Services Authority, Trading Standards Investigation Units and local authorities' Fraud Investigation Units may request SAR derived information from SOCA. These requests are risk assessed before information is disclosed.

4.15 There is an electronic 'footprint' left on ELMER when anyone has accessed a record. This applies both to internal access and those accessing ELMER via Moneyweb. The 'audit' button identifies who has accessed the record, when they have accessed the record and what they have done with the record (such as printing it out).

4.16 There is also a confidential hotline for the reporting sectors to raise concerns about the inappropriate use of SARs or breaches of SAR confidentiality. These are investigated with the end user.

4.17 SARs are routinely shared with relevant police forces based on location information. The SARs report is sent as an intelligence package. A record is kept on ELMER of who the SAR has been sent to. It is then left to the police force to decide what action to take, if any. In any event users with direct access are permitted to search, access and action SARs across the database without relying on SOCA to share the information.

4.18 Information from ELMER can also be disclosed internationally. Requests for SAR derived information from overseas Financial Intelligence Units (FIUs) are managed through the Egmont network which is a secure system. The Egmont Group is a forum for national FIUs which aims to improve international cooperation in the fight against money laundering and terrorist financing. Membership of this group means that SOCA exchanges financial intelligence with other members. Individual requests are generated through the Egmont system and consideration is given to the request and whether in fact any information can be disclosed. Information will not be shared if the country is considered to be high risk. International FIUs do not have direct access to ELMER. FIU.NET is a restricted system for sharing information between FIUs but is limited to EU members. SOCA has yet to fully exploit FIU.net. The review team were advised that concerns about whether FIU.Net meets UK standards for secure data exchange have now been resolved.

Retention

4.19 The Committee's report reflects the evidence provided to it by SOCA that each SAR is assigned a deletion date of ten years after receipt and is automatically deleted unless it has been amended or updated in which case the deletion date is reset to six years following that event. SOCA's evidence stated that there is a procedure for earlier deletion of individual SARs where all necessary activity relating to that SAR has been undertaken. The report indicated that SOCA estimates that 20,880 SARs have been permanently deleted from the database.

4.20 The review team queried the ten year retention period and what the reasoning was for this. SOCA referred to previous discussions in 1999 between the ICO (then the Data Protection Registrar) ('the Registrar') and the National Criminal Intelligence Service (NCIS) wherein the Registrar had reached an understanding with NCIS on retaining records for up to six years. The data would then be 'locked

down' for a further four years. However, as mentioned below, it seems that NCIS decided at that, in practice, it was not necessary to retain data beyond six years.

4.21 An internal NCIS memorandum dated 19 October 1999 entitled 'Procedures for deleting ELMER records' refers to discussions with the Registrar and sets out a number of recommendations in relation to when records should be deleted. It does state that the deletion procedures for ELMER have yet to be formally documented and agreed within NCIS but it is recognised that the rules for deleting ELMER records needed to be formalised although it is not clear whether this was ever done.

4.22 The recommendations were that two procedures should be adopted. Firstly, if an LEA chooses the option 'funds not linked to criminality' on the feedback form then the record should be deleted immediately 'rather than stored for 6 years'. This would be for those records where an investigation has been undertaken and found that the funds are legitimate. Secondly, it was recommended that all other records should be retained for a period of six years. The six year period would be amended if a record was updated or linked, from which point the six year period would start again. There was also a recommendation made to create an 'archiving' database which would allow for records (stripped of their underlying data) to be stored for a further four years after the six year period had expired. The 'archiving database' seems to have been decided against as it was stated that there appeared to be no benefit to having this functionality if the purpose was only for statistical analysis. Lastly, there was reference to printing out a daily report which would list all records which had one month to run before the six year period expired. This referred to reports being reviewed to determine which records should be deleted or retained for longer. This option was seen to be time consuming and burdensome but it was also acknowledged in this memorandum that the DPA could be breached if records are kept for longer than necessary.

4.23 It appears that SOCA's thinking on retention periods developed still further over time. The policy in place at the time of the review was that SARs would be deleted ten years after receipt unless there was evidence of continuing law enforcement interest in an individual SAR or more recent SARs could be linked to it and in these cases the SAR would be retained for a further six years. However, the capability to achieve this systematically has not kept pace with the increase in numbers of SARs received from 14,500 in 1999 to an estimated 250,000 in 2010. The review team found that there was no mechanism built into the system to allow 'blanket' deletion although individual cases can be deleted in some circumstances such as when there are duplicates on the system. The review team were advised that in 2011 ELMER is to undergo a rebuild to improve the processing of SARs. A project is underway to determine the requirements for the rebuild and it is intended that the final design will include a more effective automated deletion process that will enable SOCA to implement deletion rules in a more proactive and flexible way. SOCA have said that any deletion policy would need to take into account the value of older SARs and the recognition that SARs provide a defence in law to the reporter and may be subject to disclosure in Court years after they were submitted.

4.24 The review team queried whether there was any evidence of the value of data over time such as SARs being accessed which had been on the system for, say, longer than five years. It was explained by several SOCA staff that it was useful to retain the data just in case a third party needed to prove that they had submitted the SAR. There were two cases cited where it had been useful to provide evidence to show that the organisation had submitted the SAR. SOCA also provided evidence (below) to show how many times SARs received in 2004 or earlier were accessed by end users during each month in 2009 -

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	
1994	139	172	105	84	141	148	137	150	107	117	123	81	1,504
1995	157	175	141	125	122	138	204	138	116	141	128	85	1,670
1996	98	80	61	63	73	113	102	70	81	64	47	36	888
1997	94	96	71	86	84	92	97	68	82	74	47	47	938
1998	103	89	94	93	93	129	104	80	67	80	123	116	1,171
1999	196	147	150	146	176	169	188	151	164	131	233	75	1,926
2000	265	333	281	216	248	215	337	269	227	343	348	189	3,271
2001	480	479	441	433	400	484	544	406	525	720	395	435	5,742
2002	1,365	1,183	1,180	1,104	1,134	1,447	1,600	1,049	1,114	1,479	1,492	832	14,979
2003	3,653	2,483	2,414	1,797	2,347	3,442	2,166	1,870	1,906	2,364	2,323	1,645	28,410
2004	4,777	3,593	3,676	2,374	3,790	4,310	3,046	2,648	2,342	2,928	2,500	1,681	37,665
Totals:	11,331	8,838	8,616	6,521	8,611	10,688	8,526	6,899	6,731	8,442	7,765	5,222	98,190

Source: SOCA

It should be noted that the table shows that the records were 'hit' but does not provide any further detail than that. It is possible that some of the aged hits may have occurred when searching on similar names and not because of concerns about unlawful activity by that person. It is notable that the number of checks drops substantially when records are over seven years old.

Governance

4.25 The SARs Regime Committee was set up to supervise SOCA's discharge of its responsibilities with regards to the SARs Regime. The Regime Committee is a committee of the SOCA Board and has terms of reference in place. The Regime Committee comprises members from the reporting sectors, regulators, professional bodies and from end users as well as the SOCA FIU management.

4.26 There is a comprehensive set of policies and procedures governing the SARs regime which the review team has had sight of.

4.27 The governance arrangements also include a substantial number of documents which include the SARs Annual Report, Home Office Guidance on the Handling and Confidentiality of SARs (HO Circular 53/2005) and the twice yearly Feedback Questionnaire. This provides a mechanism for the regular exchange of information with end users/reporters.

5. Conclusions

5.1 The level of co-operation from staff at SOCA was exemplary. All the staff the review team met were clearly committed to the work that they do.

5.2 The review team found that there were many examples of good practice. The automatic keyword search which is undertaken when a SAR is received means that those SARs which could be of concern are flagged up automatically. This helps alleviate concerns about SARs going straight onto ELMER without consideration.

5.3 The review team also found that the proactive sharing of SARs with relevant police forces was helpful to ensure effective scrutiny of the records.

5.4 The security, policy and procedures in relation to SAR Online appear sufficiently robust. Access to ELMER is tightly controlled and unused accounts are reviewed and deleted if necessary. Direct access to ELMER is also not as widespread as had first been suggested.

5.5 The audit trail on ELMER was also reassuring. Not only did the 'audit' facility indicate who had accessed a particular record (both internally and externally) but it could be seen what had happened to the record for example if it was printed out.

5.6 However, whilst those SARs of concern are flagged and considered (either within SOCA or externally when divulged to the relevant LEA) those that raise no concerns are in effect retained indefinitely. This raises compliance concerns and the review team were not satisfied that there was currently sufficient evidence to support the long retention of SARs of no concern. It was also clear that the current system does not support the existing retention policy in practice.

5.7 There are several aspects of the operation of ELMER which raise concerns about compliance with the Data Protection Act. The first data protection principle states that personal data shall be processed fairly and lawfully. Central to this is the requirement that individuals have an understanding of how their personal information will be processed by those who hold it. The Commissioner is concerned whether these fair processing requirements are being met in those cases of no concern retained on a system indefinitely without the knowledge of those individuals to whom those reports relate. The third principle requires that personal data shall be adequate, relevant and not excessive. The fifth principle requires that

personal data should not be kept for longer than is necessary. The Commissioner takes the view that that the current arrangements governing the retention of records, particularly those records that raise no concerns, may not comply with these requirements.

5.8 The first principle also requires that personal data are processed fairly and lawfully. This lawful processing element requires consideration of whether the processing of SARs is compliant with other legal duties. SOCA is required to comply with the provisions of the Human Rights Act 1998 which gives effect in the UK to the European Convention on Human Rights. Article 8 of that Convention is engaged by the processing of SARs and its provisions together with the jurisprudence of the European Court of Human Rights (ECtHR). The retention of data on the ELMER database engages concerns about whether this is an unjustified interference with an individuals' right to respect for their private and family life, particular taking into account the judgment of the ECtHR in the 'S and Marper'[18] case.

5.9 The retention of SARs which raise no ongoing law enforcement concerns and the retention of these for an indefinite period engage concerns about out whether such retention is justified, necessary and proportionate. It is difficult to conclude that this is the case.

5.10 Given that compliance with ECHR obligations is in question, this also calls into question whether such personal data are lawfully processed in accordance with the requirements of the first principle.

5.11 Further, apart from the Committee's Inquiry there has been little in the way of post-legislative scrutiny of the relevant legislation which introduced the requirement to report suspicions to SOCA. The current law focuses on reporting but there are no additional safeguards on the face of the legislation to prevent the disproportionate retention or to prevent reporting of cases likely to be of little or no interest. The Commissioner's view is that any legislation which engages significant privacy concerns should include on the face of it a requirement on the Government to report to Parliament on how the measures have been deployed including evidence of the extent to which the expected benefits and possible risks have been realised in practice and the continued need for the measures in question.

6. Recommendations on future action

6.1 The Commissioner makes a number of recommendations to help ensure that the processing of personal data on the ELMER database complies with the requirements of the Data Protection Act and on the legislative approach to the reporting of suspicious financial activity. These are set out below:

6.1.1 That SOCA continues to maintain its current robust policies and procedures in respect of access to ELMER, the automatic keyword search, the proactive sharing of SARs with LEAs and the security of SAR Online. This will be particularly important in the context of the proposed changes affecting SOCA outlined in the Government's recent 'Policing in the 21st Century' consultation.

6.1.2 That SOCA develops, implements and actively manages a record retention and deletion policy which addresses the requirements of the DPA and HRA on necessity and proportionality. This policy should be developed in consultation with the Commissioner.

---

[18] S and Marper v United Kingdom [2008] ECHR 30562/04 [Grand Chamber] (4 December 2008)

6.1.3 That SOCA develops a plan for the development and implementation of a DPA and HRA compliant retention policy within three months of the presentation of this report.

6.1.4 That SOCA ensures that the planned upgrade of ELMER includes the functionality to support the new record retention policy and that this is introduced during 2011.

6.1.5 That the Government considers whether, in the light of experience, the current arrangements for reporting of SARs continue to be justified, whether they are both effective and proportionate and whether they could be improved. Consideration should be given to whether there is a pressing social need to justify the requirement to report any transaction which is based on a very low threshold of suspicion that handling criminal property or money laundering is taking place.

Annex 1: The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Annex 2: Relevant legislation

1. European Directives

(i) 91/308/EEC—Incorporated into UK law via the Criminal Justice Act 1991, the Drug Trafficking Act 1994 and the Money Laundering Regulations 1993.

(ii) 2001/97/EC—Incorporated into UK law via the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003.

(iii) 2005/60/EC—Incorporated into UK law by the Money Laundering Regulations 2007, the Terrorism Act 2000 (Amendment) Regulations 2007 (TACT Regulations 2007), Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (POCA Regulations 2007).

2. Serious Organised Crime and Police Act 2005 (SOCPA)—enacted SOCA assuming responsibility for the national FIU.
3. Serious Crime Act 2007
4. Anti-Terrorism Crime & Security Act 2001
5. Counter Terrorism Act 2008
6. EU Regulation on Counter Proliferation Finance

APPENDIX 3: LETTER FROM LORD ROPER TO LORD SASSOON, COMMERCIAL SECRETARY TO THE TREASURY

Information Commissioner's report to the House of Lords European Union Committee on SOCA's operation and use of the ELMER database

You will remember that the Home Affairs Sub-Committee of the House of Lords Select Committee on the European Union carried out an inquiry last year into the part played by the EU in countering money laundering and the financing of terrorism. As a former President of the FATF you kindly gave evidence to that inquiry. It resulted in the report *Money laundering and the financing of terrorism* (19th Report, Session 2008–09, HL Paper 132).

You will recall that the Committee was concerned about the width of access to ELMER, the database of suspicious activity reports kept by SOCA. We recommended that the Information Commissioner should review and report on the operation and use of this database. The Information Commissioner has now completed this review, and has reported to the Committee. We are most grateful to him for this review, which seems to justify our own view that the database is not fully compliant with the Data Protection Act or the Human Rights Act, and that steps could and should be taken to remedy this.

We intend to make a brief report to the House of Lords in January to which we will append the Information Commissioner's report. However the majority of his recommendations are addressed to SOCA and to the Government. I therefore attach a copy of his report to enable you to consider his recommendations. I look forward to hearing in the course of January your reaction to them.

15 December 2010 ROPER