UK Law Enforcement Agency Use and Management of Suspicious Activity Reports: Towards Determining the Value of the Regime

Matthew H. Fleming*
(University College London)

30 June 2005

* Research Fellow, Jill Dando Institute of Crime Science, University College London. Author's email address: m.fleming@ucl.ac.uk. Opinions expressed herein are those of the author and do not necessarily represent those of University College London.

[Blank page]

Contents Page

Acronyms iii

Acknowledgements iv

Executive Summary v

I. Introduction 1

II. Background 3
- A. SARs from Disclosure to LEAs: An Overview 3
- B. Scope of the Problem 8
- C. Methodology 11

III. Theory: SARs from Information to Intelligence to Outcomes 13

IV. Findings 20
- A. UK LEA Use and Management of SARs 20
  1. Users of SARs 21
  2. Management of SARs (Processes) 25
  3. Uses of SARs (Outcomes) 29
  4. Feedback from LEAs to NCIS/Industry 42
  5. The System in Flux 46
- B. The Experiences of Overseas Jurisdictions 53
- C. The Regulated Sector and Its Desires for Feedback 58

V. Discussion and Recommendations 63

VI. Conclusion 73

References 74

Appendix I: SARs Case Examples Provided by LEAs 78

Appendix II: Examples of Good Practice in SARs Management (Processes) 82

Figures
1. Annual and Monthly SARs Receipts by NCIS, 2003-2004 4
2. SARs Receipts by NCIS by Sector, September 2003-December 2004 5
3. Monthly Receipts and Disseminations of SARs by NCIS, January 2003-April 2005 52

Tables
1. Uses of SARs in an Intelligence Context 17
2. Primary Users of SARs (with 2003-2004 Annual Allocations and Disseminations) 22
3. Annual Receipts and Disseminations of SARs by NCIS to LEAs, 2003-2004 30
4. Annual Nonconsent and Consent Outcomes Metadata, 2003-2004 31
5. Annual Nonconsent and Consent Outcomes, 2003-2004 35
6. Annual Nonconsent Investigative Processes for 14 LEAs, 2004 36
7. Annual SARs-Related Cash Seizures and Confiscations as a Percentage of Cash Seizures and Confiscations, 2004 37
8. Database Hits on a Sample of SARs from a London Borough 39
9. PNC Hits on a Sample of SARs from the MPS FIDU 39

10. SAR Feedback Form 43
11. Annual Feedback Sent from LEAs to NCIS, 2003-2004 44
12. Annual SARs and Workloads by LEA, 2004 48
13. SARs/FTRs in Australia, Canada, the United Kingdom, and the United States 55
14. What Sort of Systematic Feedback Does the Regulated Sector Want to See 59
15. Recommendations 71

ACRONYMS

ACPO	Association of Chief Police Officers of England, Wales, and N. Ireland
ACPOS	Association of Chief Police Officers of Scotland
AML	Anti-Money Laundering
ARA	Assets Recovery Agency
AUSTRAC	Australian Transaction Reports and Analysis Centre
CFT	Combating the Financing of Terrorism
CICFA	Concerted Interagency Criminal Finances Action Group
DWP	Department of Work and Pensions
Elmer	The NCIS SARs database
FATF	Financial Action Task Force
FI	Financial Investigator
FIB	Force Intelligence Bureau
FID	Financial Intelligence Division of NCIS (now known as SFI)
FIDU	Financial Intelligence Development Unit
FinCEN	Financial Crimes Enforcement Network (USA)
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Investigation Unit
FIWG	Financial Investigator Working Group
FSA	Financial Services Authority
FTR	Financial Transaction Report
HMCE	Her Majesty's Customs and Excise
HMIC	Her Majesty's Inspectorate of Constabulary
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
IMF	International Monetary Fund
IR	Inland Revenue
JARD	Joint Asset Recovery Database
JDI	Jill Dando Institute of Crime Science, University College London
JMLSG	Joint Money Laundering Steering Group
LEA	Law Enforcement Agency
MLAC	Money Laundering Advisory Committee
MLRTF	Money Laundering Reporting Task Force
MPS	Metropolitan Police Service
NCIS	National Criminal Intelligence Service
NCS	National Crime Squad
NIM	National Intelligence Model
NTFIU	National Terrorist Financial Investigation Unit (Special Branch)
PITO	Police Information Technology Organisation
PIU	Performance and Innovation Unit, Cabinet Office
PNC	Police National Computer
POCA	Proceeds of Crime Act 2002
PSNI	Police Service of Northern Ireland
RART	Regional Asset Recovery Team
SAR	Suspicious Activity Report
SDEA	Scottish Drug Enforcement Agency
SFI	Services-Financial Intelligence (formerly FID, the NCIS SARs-handling unit)
SOCA	Serious Organised Crime Agency
TFT	Terrorist Finance Team (NCIS)

ACKNOWLEDGEMENTS

This research is the result of four+ months of intensive work. It would not have been possible without the generous assistance of a large number of people and organizations. In particular, I would like to thank Nigel Coles, David Thomas, Kevin Higgins, and Oliver Higgins of NCIS (and their numerous colleagues who provided so much useful insight and information); Roger Aldridge, ACPO Lead on Proceeds of Crime Issues (whose support, through ACPO, was invaluable); Jim Bradley and Robert Lawman of the Home Office; Tim Harvey of the City of London Police and Chair of the National Financial Investigator Working Group (whose ability to encourage police forces to respond to the survey was unparalleled); Jane Earl and Charlie Dickin of ARA; Kate Flannery and Neville Pinkney of HMIC; Lucy Makinson and Ian Mynot of HMT; Tristram Hicks of the London Regional Asset Recovery Team; Sara Thornton, ACPO Lead on Intelligence Issues; Jeremy Outen, Adam Bates, and Gus MacKenzie of KPMG, not least for the very generous use of their data and their learned input; Robin Booth of BCL Burton Copeland; Steve Lock of Prudential; John Mair of Lloyds TSB; Karen Silcock of Deloitte; Kathy Woodfine of Goldman Sachs; Carol Prasad and Wendy Ward of AUSTRAC; Joanna Brown and Deborah Silberman of FinCEN; Debra Cowie of FINTRAC; and Gloria Laycock of University College London. Indeed, a long list of individuals from government, the private sector, and law enforcement (within the UK and overseas) contributed to this project. There simply isn't enough space to list them all. I remain indebted to them—for their considerable time, expertise, and information (much of which had not been previously released to the public)—and hope that this report is of some assistance to their endeavours. But a last special thank you goes to the LEAs who participated in this research, representing nearly the entire UK SARs user community. Their excellent, thoughtful, selfless cooperation will not soon be forgotten.

EXECUTIVE SUMMARY

A suspicious activity report (SAR) is a piece of information which alerts law enforcement that certain customer activity is in some way suspicious and might indicate money laundering or terrorist financing (and thus criminal and/or terrorist activity). SARs are sent by members of the regulated sector to the National Criminal Intelligence Service for processing, and are subsequently passed to law enforcement agencies (LEAs) for action. But the extent to which SARs are actually used by law enforcement (and the value of SARs to law enforcement) has not been entirely clear. As such, the Jill Dando Institute of Crime Science, University College London, carried out an intensive four-month research project on the regime, commissioned by ACPO, funded by the Home Office, and with the support of NCIS. The research aimed to provide systematic information on the use and management of SARs in law enforcement agencies in the UK, to identify gaps in that information, and to propose actions to bridge such gaps. By design, much of the information contained in this report is historical in nature. But this should in no way imply that the information is of lesser relevance: for one thing, industry and policy-makers have a right to know what the SARs regime has accomplished. Moreover, understanding the evolution of certain policies and procedures and their impact on LEA performance—and learning from past mistakes and successes—are critical to the effective and efficient functioning of the regime. Lastly, despite an outward emphasis on LEAs, NCIS figures prominently in the report. This is the case because 1) NCIS itself is a user of SARs; and 2) LEA use and management of SARs are entwined with the SARs-related policies and procedures of NCIS.

Principal findings of the research are as follows:

Despite evidence of some important SARs-related successes, SARs appear to be under-utilised by most LEAs. This is not to suggest that *all* LEAs are under-performing on SARs; a number of LEAs appear to be carrying out some good work with SARs (both proactive and reactive). And all LEAs appear to do at least *something* with SARs. But the available data—admittedly of low quality and limited depth—*coupled with the admissions of LEAs themselves* together suggest that SARs could be better and more frequently utilised. A number of factors were identified which appear to contribute to this under-utilisation, including the following (though not all will be relevant for each and every LEA):

- LEAs appear to have insufficient resources to develop and exploit the information contained in SARs.
- SARs-development units (typically FIUs) often view confiscation and cash seizure as competing with SARs for scarce resources (even though the work is very likely complementary).
- SARs-based cases are difficult to sell to operational teams.
- IT systems commonly used allow for only limited SARs-related analyses.
- SARs may contain unclear reasons for suspicion or may relate to noncriminal activity (i.e. disclosures may be incomplete and/or represent mistaken suspicion or purely defensive reporting).

- LEAs receive little guidance/training/advice on the use of SARs.
- Few carrots or sticks drive the use of SARs: no performance indicators encourage LEAs to make proactive/reactive use of SARs (and only things which are measured appear to get done).
- Along these lines, there is no larger accountability for either LEAs or NCIS on the use of SARs; the regime has no real owner to encourage solid performance, to effect change, and to coordinate the SARs-related activity of numerous government departments and agencies. Neither is there a mission statement which clearly sets out the aims of the regime.

Furthermore, systematic information maintained by LEAs on their use of SARs is limited and often of poor quality. This appears to be the case because:

- LEAs employ limited if any case management systems or approaches (or if such systems are employed, limited IT fluency prevents statistics from being produced).
- Insufficient LEA resources limit the availability of systematic management information.
- Many LEAs claim to be unaware of the statistical indicators which might be of interest to industry and the larger policy community.
- And some LEAs may exhibit a disdain for record-keeping.

Some systematic information on the use of SARs is, of course, maintained by LEAs. **But this information—particularly the feedback provided to NCIS—is under-utilised by NCIS and subsequently by industry and the larger policy community**.

Additionally, communication/feedback between and within LEAs, NCIS, ACPO, government, and industry is suboptimal.

Lastly, on a positive note, change is afoot in the SARs regime—especially with the rollout of the Elmer database and the creation of SOCA. The rollout of the Elmer database will greatly facilitate the use of SARs. The creation of SOCA, as a break from the past, presents a rare opportunity to right many of the wrongs of the regime in one fell swoop.

The research makes 15 recommendations for action. All should improve LEA use and management of SARs and should allow for systematic information to be captured by LEAs, assembled by NCIS, and consumed by industry and policy-makers. Notably, some of the recommendations have been made in the past by various sources. Recommendations are classified as *critical*, *highly desirable*, and *desirable*.

Recommendations are as follows:

Recommendation 1 (critical). For accountability purposes and to coordinate the activities of the various relevant government departments and agencies, the SARs regime should once and for all be assigned an "owner" (most likely NCIS/SOCA with a slightly expanded remit), and this owner should be governed by an oversight board.

Recommendation 2 (critical). The first task of the regime's owner (NCIS/SOCA)—in conjunction with all of the relevant parties within the regime (e.g. ACPO/ACPOS, HMRC, Home Office, HMT, FSA, CICFA, and perhaps MLAC)—should be to publish a mission statement that sets out the aims, objectives, and principles of the SARs regime.

Recommendation 3 (critical). LEAs should make constant, unwavering use of the Elmer database, including the feedback mechanism.

Recommendation 4 (critical). In accordance with the aims of the regime—and to encourage constant and unwavering LEA use of Elmer—LEAs should be given guidance on what is expected of them in the form of nationally-agreed minimum work standards on the use of SARs generally, the use of Elmer specifically, and the provision of feedback/statistics. Performance indicators should be introduced which mirror these minimum standards. Minimum standards should be assembled by the owner of the regime (NCIS/SOCA) in conjunction with ACPO/ACPOS, HMRC, the Home Office, ARA (given its training responsibilities), and perhaps SDEA, DWP, and NCS.

Recommendation 5 (critical). To encourage take-up of minimum work standards (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should monitor LEA access to Elmer and maintain management information on account logins, database searches, and SAR downloads. This information should be reported to LEA managers, as well as ACPO/ACPOS, HMRC, and the Home Office

Recommendation 6 (critical). For similar accountability purposes (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should make systematic use of the feedback provided by LEAs on their use of SARs. This information should be reported to LEA managers, as well as ACPO, ACPOS, HMRC, and the Home Office.

Recommendation 7 (critical). Because of associated efficiency gains for users of SARs, NCIS/SOCA should ensure that Phase II of the Elmer rollout—with its advanced analytical capabilities—is delivered on schedule.

Recommendation 8 (critical). Because of associated efficiency gains for users of SARs, database cross-checks between Elmer and relevant national databases (e.g. PNC, JARD) should be automated, such that database hits are highlighted when looking at a SAR or series of SARs on Elmer; this should be handled by NCIS/SOCA, perhaps in conjunction with the Police Information Technology Organisation (PITO).

Recommendation 9 (critical). LEAs, particularly those with the most limited SARs-related capacity, should devote greater staffing resources to units with responsibility for SARs; resources should be ring-fenced if possible.

Recommendation 10 (highly desirable). JARD should be modified to capture information on whether or not SARs initiated or otherwise played a role in cash seizures and confiscations.

Recommendation 11 (highly desirable). ACPO should decide who exactly within police LEAs will have access to Elmer: FIUs, FIBs, or both—and how.

Recommendation 12 (highly desirable). The regime's owner (NCIS/SOCA) should publish an annual report on the SARs regime (drawing on the use of SARs by LEAs) and make it freely available via the internet.

Recommendation 13 (highly desirable). The regime's owner (NCIS/SOCA) and its LEA partners should ensure that lines of communication on SARs-related issues are open and functioning effectively.

Recommendation 14 (desirable). ACPO/ACPOS and the Home Office should strongly encourage LEAs to employ case management systems which allow LEA personnel to follow the progression of a case from the intelligence development stage to final outcomes—unless effective systems are already in use—to facilitate Elmer feedback and deeper analysis of SARs.

Recommendation 15 (desirable). An in-depth follow-up study on LEA use and management of SARs similar to the present research should be conducted in 2006 or 2007 to track progress on use of SARs. This is relevant especially with the rollout of Elmer, which will fundamentally change the interface between LEAs and SARs.

I. INTRODUCTION

1. A suspicious activity report (SAR) is a piece of information which alerts law enforcement that certain customer activity—perhaps a series of large out-of-character deposits or the cash purchase of a high-value asset—is in some way suspicious and might indicate money laundering or terrorist financing (and thus criminal and/or terrorist activity). SARs are sent by members of the regulated sector (e.g. banks and building societies, law firms, accounting firms) to the National Criminal Intelligence Service (NCIS) for processing, and are subsequently passed to law enforcement for action. The SARs regime, which has been in place since legislation was introduced in 1986, has undergone significant recent legislative modification: the Proceeds of Crime Act 2002 (POCA) and the Money Laundering Regulations 2003 redefined the offence of money laundering and captured a broader range of activity within the business of the regulated sector. The number of reports received has grown considerably in the past several years; some 56,000 were received in 2002, nearly 95,000 in 2003, and more than 154,000 in 2004. Regulated sector compliance with the regime is mandatory.

2. But the extent to which SARs are actually used by law enforcement (and the value of SARs to law enforcement) has not been entirely clear. A July 2003 KPMG report commissioned by NCIS revealed significant shortcomings with the regime and suggested 21 recommendations to carry it forward. While many recommendations have been taken on board by appropriate agencies, unease with reporting requirements has been registered by the regulated sector, primarily because law enforcement agencies (LEAs) continue to have poor management information on how SARs are actually used. A mid-2004 position piece of the Association of Chief Police Officers of England, Wales, and Northern Ireland (ACPO) put it this way: "As the requirements of POCA come into force in respect of Suspicious Activity Reporting, there is increasing concern from those industry sectors required to report, that the reports are not actioned by police and other law enforcement agencies, such that they question the need for the requirement as it currently stands…they seek some reassurance from law enforcement on the use of the information they are providing" (Aldridge, 2004).

3. As such, the Jill Dando Institute of Crime Science, University College London (JDI), carried out an intensive four-month research project on the regime, commissioned by ACPO, funded by the Home Office, and with the support of NCIS. The research aimed to provide systematic information on the use and management of SARs in law enforcement agencies in the UK, to identify gaps in that information, and to propose actions to bridge such gaps. Building on the findings of the 2003 KPMG report, the research sought to answer the following questions: To what extent are SARs currently being used by LEAs? Do (and can) SARs appear to contribute to crime reduction in a meaningful way, and if so, how? What can be done, particularly to the way in which LEAs manage SARs, to increase the likelihood that law enforcement, policy-makers, and industry can make informed judgments about SARs' contribution to crime reduction?

4. This paper sets forth the findings of the research. It is structured as follows: after this introduction, a background section presents an overview of the regime, the scope of the problem, and the methodology of the study; the theoretical underpinnings of SARs are discussed, including their role in crime reduction in the context of intelligence; the findings are presented; a discussion section examines the implications of the research and sets forth recommendations for action; and a conclusion brings things to a close. Case

examples of the use of SARs by LEAs are found in an appendix, as are examples of good practice in SARs management employed by LEAs. Finally, note that the concept of law enforcement used in this report is a broad one, and includes the law enforcement arms of various non-police organisations (e.g. Department of Work and Pensions). Note also that Her Majesty's Customs and Excise (HMCE) and Inland Revenue (IR) became Her Majesty's Revenue and Customs (HMRC) on 18 April 2005. This research refers to HMCE and IR as separate entities as appropriate (e.g. with historical uses of SARs).

II. BACKGROUND

A. SARs from Disclosure to LEAs: An Overview[1]

5. As set forth in POCA, SARs are filed by entities in the regulated sector when they have knowledge or suspicion of money laundering activity (or have reasonable grounds to know or suspect such activity).[2] Money laundering activity is set forth in Sections 327, 328, and 329 of POCA; it includes the concealing, arranging, and acquisition (acquisition, use, and possession) of criminal property. The regulated sector includes banks/building societies, accountants, lawyers, estate agents, casinos, money service bureaux, and dealers in high-value goods. Failure by a regulated sector entity to disclose money laundering activity (through a SAR) is itself a crime. A SAR captures information which includes subject details (i.e. information regarding the subject(s) of the disclosure, be it an individual or legal entity), transaction details with account information, and the reason for disclosure (i.e. for suspicion). SARs are also filed to secure law enforcement consent on future activity which may constitute a prohibited act (e.g. the transfer of funds suspected of being criminal property). Of the 154,536 SARs received by NCIS in 2004, nearly ten percent were consent SARs (this report will refer to *nonconsent* and *consent* SARs throughout). Banks/building societies file more than 75 percent of nonconsent SARs; the legal profession accounts for more than 80 percent of consent SARs, though this will likely fall with the recent Bowman v. Fels judgment.[3] See Figures 1 and 2, below, for information on receipts of SARs by NCIS.

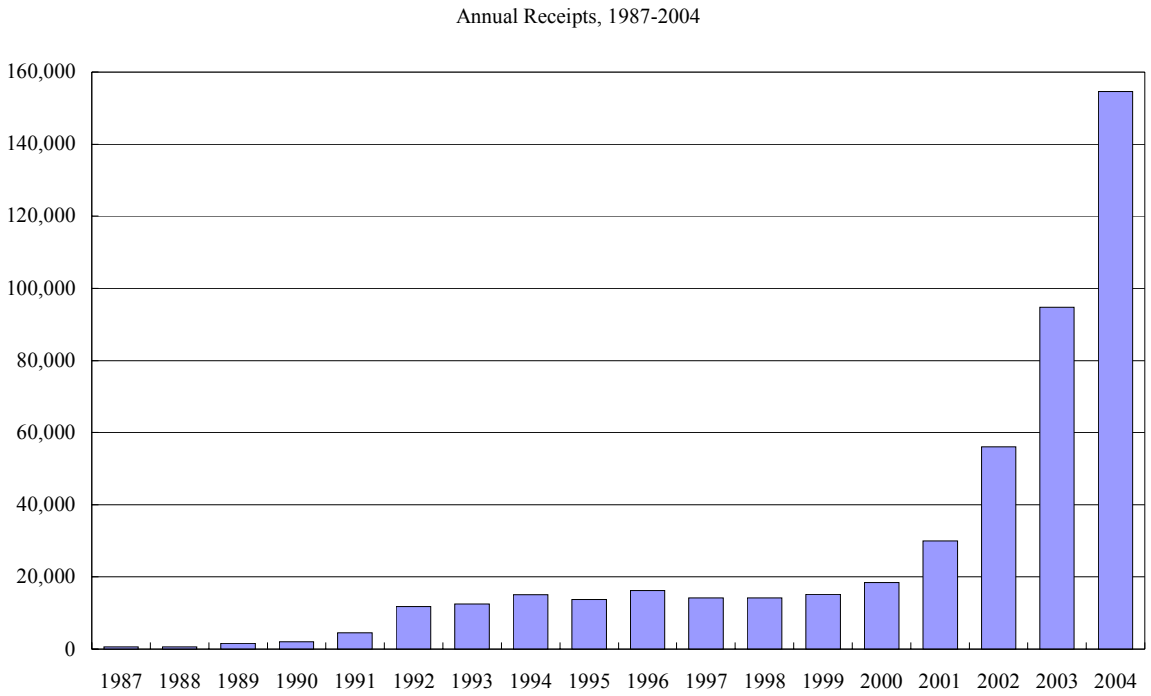
---

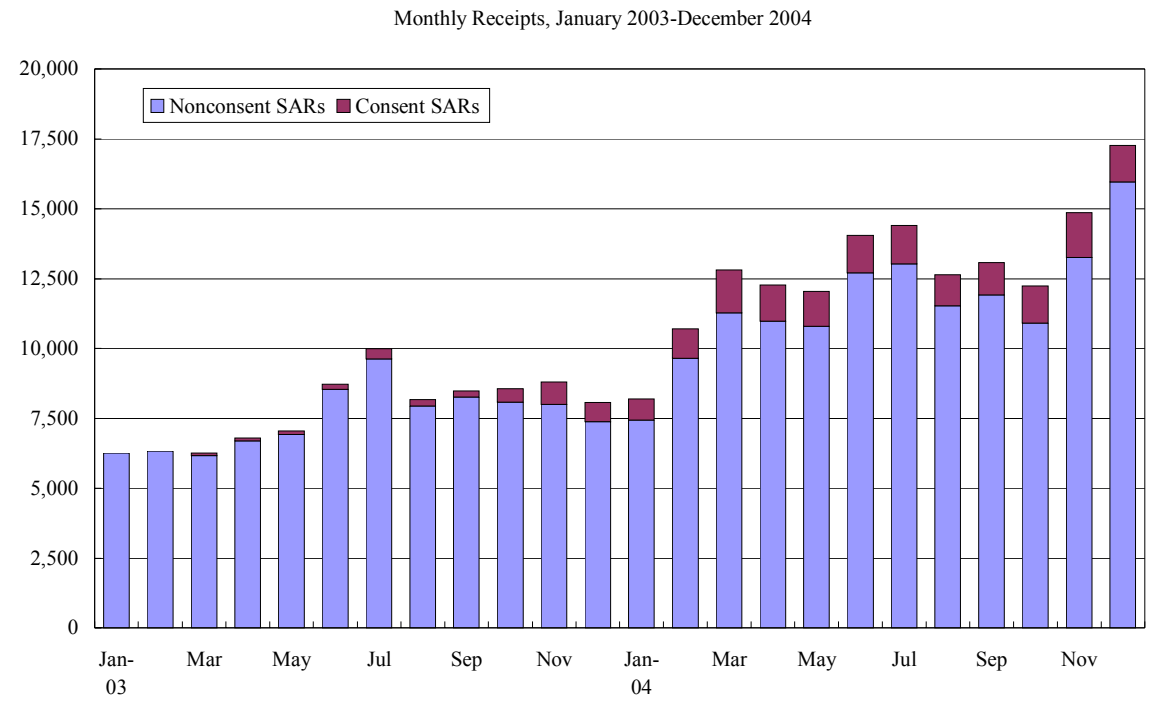
[1] Much has been written on the regime over the years. For historical perspectives and process-related information, see, for example, KPMG (2003), PIU (2000), and/or Gold and Levi (1994), though because of the rate of change, even KPMG is to some extent dated. HMT (2004) provides a broad summary of the UK's AML strategy. The Joint Money Laundering Steering Group (JMLSG) *Guidance Notes* provide a comprehensive summary of the regime, though with an industry focus. The *Guidance Notes* are currently undergoing a significant revision; the latest draft is publicly available at < http://www.jmlsg.org.uk/>.

[2] SARs are distinct from the threshold-based reports employed in a number of overseas jurisdictions. The term *SAR* is not used in POCA. POCA requires businesses in the regulated sector to make a disclosure; this disclosure is commonly known as a SAR.

[3] According to the Law Society, the Bowman v. Fels ruling "makes clear that legal professional privilege places solicitors under a primary duty to the court and their client, exempting them from making money laundering reports when acting in litigation" (Law Society, 2005).

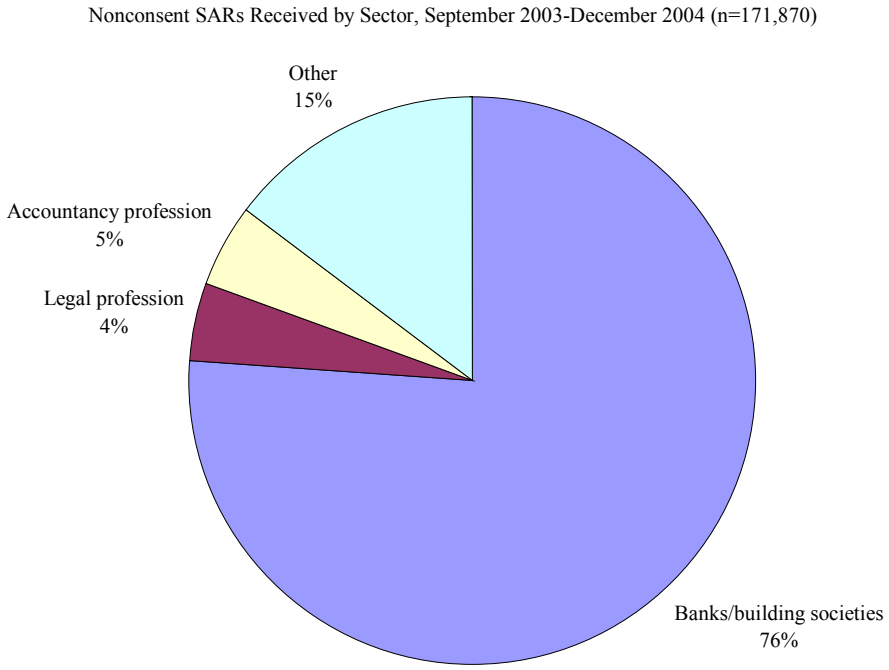
Figure 1. Annual and Monthly SARs Receipts by NCIS

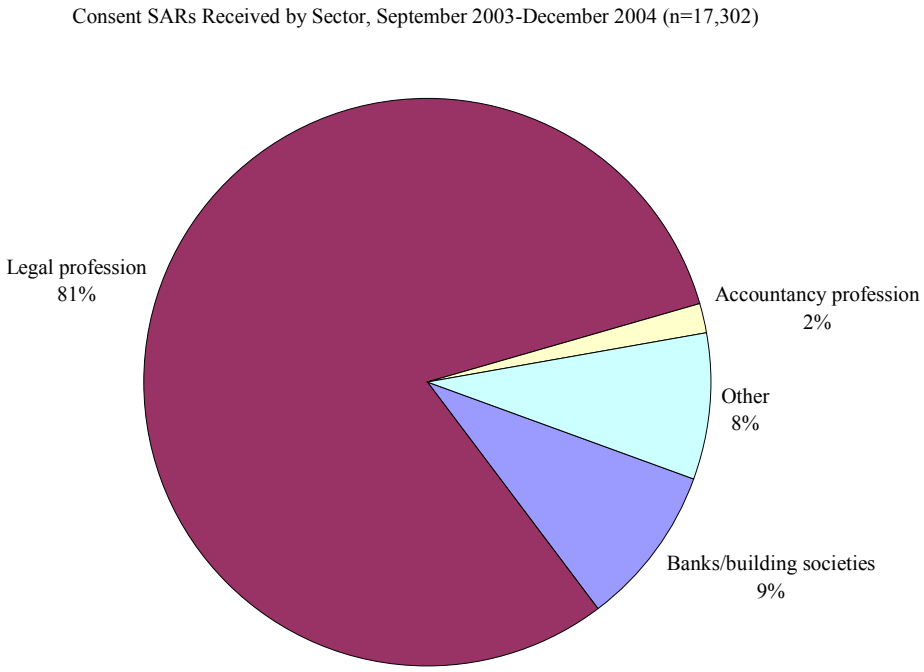




Source: NCIS. Based on receipts from January-April 2005, total 2005 annual receipts should be on the order of 165,000.

Figure 2. SARs Receipts by NCIS by Sector





Source: NCIS. Note that no sectoral breakdowns are available prior to September 2003. Percentage receipts by sector are broadly stable over time. The legal profession's share of consent SARs should fall due to the Bowman v. Fels ruling of March 2005.

6. SARs are sent electronically (via internet or fax) or in hard copy to NCIS.[4] Once received, SARs are input into Elmer, the SARs database, and may undergo cursory analysis (analysis of individual SARs has evolved over time).[5] But while NCIS may develop intelligence packages and products, it does not itself make arrests. As such, SARs and other forms of criminal intelligence, not discussed here, are sent from NCIS to LEAs for action. Note that an important distinction is drawn for the purposes of this paper between the words *allocate* and *disseminate*: SARs are automatically *allocated* (i.e. assigned) to an appropriate LEA by the Elmer system; SARs are *disseminated* when they are actually sent to LEAs for action. All SARs are allocated, but not all SARs are disseminated, at least at present. The manner in which SARs are disseminated to LEAs (including what has been done to those SARs sent, and what percentage of the total is sent out) has changed significantly since publication of the KPMG report. The process can be divided into four distinct periods: pre-July 2003 (pre-KPMG); July 2003-June 2004; June 2004-Elmer rollout in May 2005; post-rollout.[6]

- **Pre-July 2003**: Prior to the release of the KPMG report in July 2003, all SARs upon receipt were searched against the Alert database (the NCIS database of level 3 targets, now known as Elementary) and Elmer itself. If there were database hits, the SAR was allocated and disseminated to the interested LEA as recorded on Alert/Elmer. If there were no hits, the SAR was allocated and disseminated to the relevant LEA by postcode. Additionally, staff from organisations including HMCE, IR, and the Terrorist Finance Team (TFT) sited at NCIS actively combed the Elmer database for work appropriate to their respective organisations (and to the National Terrorist Financial Investigation Unit of Special Branch, NTFIU, in the case of the TFT). All SARs were disseminated. SARs were sent out via email in "LEA packs" which contained the SAR, comma separated variable format of the SAR data (CSV format can be easily pulled into a variety of database and spreadsheet applications, like Microsoft Excel), a feedback form, and information on links to previous SARs (including previous SAR numbers and to whom/when they were disseminated). SARs needing immediate action (as judged by the Duty Desk) were fast-tracked to the relevant LEA; non-fast-track SARs were processed with lower priority. There were often delays in the dissemination of non-fast-track SARs of several months if not more (KPMG, 2003).[7]

---

[4] At present, there are no prescribed forms on which SARs must be sent to NCIS. NCIS encourages filers to use either the Standard Disclosure Report Form or the Limited Intelligence Value Report Form, both available at http://www.ncis.co.uk/disclosure.asp. Further, there is no prescribed manner in which filers must report, though reporting entities are encouraged to use bulk submission or the *money.web* extranet.

[5] Not all SARs are input on Elmer, though NCIS is moving to rectify this. As at March 2005, some 15,000 SARs were awaiting input; as at May 2005, this was reduced to some 3,000 SARs. Mandatory electronic reporting and prescribed forms would lighten resource demands to some extent.

[6] Changes in the dissemination process carry implications for the present project. The research examines both historical information (i.e. the extent of recent use and management of SARs and deficiencies in management information) and the manner in which the Elmer rollout may affect LEA activity.

[7] At the time of its assessment of the UK's AML regime in 2002, the IMF found evidence of NCIS processing/analysis taking three months (IMF, 2003). Participants in Operation Kinloss, a May 2002-March 2003 Home Office-funded project intended to explore the benefit of employing ring-fenced SARs personnel, found evidence of SARs taking more than one year from disclosure to receipt by an LEA (Hicks, 2003).

- **July 2003-June 2004**: Following the release of the KPMG report and until June 2004, all SARs were individually assessed on a qualitative basis and according to the intelligence requirements of LEAs and NCIS itself. SARs assessed to be of interest were disseminated to the relevant LEA by postcode as per intelligence requirements; those which did not, through assessment, meet dissemination criteria were retained on-site (i.e. kept in the Elmer database, but not disseminated). The SARs assessed as fit for dissemination were searched against Alert and Elmer, and, occasionally, a search would be conducted on the Police National Computer (PNC) or HMCE's Cedric (now known as Centaur). As with the pre-KPMG period, staff from various agencies continued to work onsite; fast-track SARs were given higher priority in processing; and SARs were sent out via the LEA packs. Delays in the processing of non-fast-track SARs persisted.

- **From June 2004 to the Elmer rollout (end-May 2005)**: With little fanfare—and with no apparent consultation with LEAs—NCIS significantly reduced the volume of dissemination of SARs to LEAs in June 2004. Staff from IR and TFT, (but no longer HMCE) still comb the database for their organisations, and three LEAs (Cheshire Constabulary, Merseyside Police, and the Metropolitan Police Service) receive semi-regular CD-ROMs with unprocessed, unevaluated raw SARs data.[8] LEAs are encouraged to submit Elmer search requests (these have been available since well before KPMG, but their use has become all the more relevant). Those SARs which are indeed disseminated have likely been identified by IR or TFT; have been highlighted for further scrutiny through daily target and keyword searches of the database; may support a specific law enforcement initiative like Operation Payback; or are the result of NCIS analyses (e.g. searches for the most-disclosed-upon individuals) and/or product development. The disseminated SARs are still searched against Elementary, and links to other SARs are still identified (though this may not happen in all cases: support to Operation Payback and/or lists of the most-disclosed upon individuals may go out as lists of names/addresses). To explain the change in procedure, NCIS states that "the previous practice of wholesale allocation of single SARs, on a reactive basis, has been replaced with the delivery of intelligence assessments, prioritised subjects lists and targeted SARs" (NCIS, 2005), and that "the reactive, one by one allocation process risked not revealing the most capable and most prolific of money laundering suspects and not highlighting patterns and typologies" (NCIS, 2004).

- **Post-rollout**: On 27 May 2005, LEAs should have remote read-only, semi-searchable online access to the Elmer database.[9] Elmer will be delivered via the *money.web* extranet. All SARs will be accessible to all registered users nationwide (with the exception of SARs in certain categories, including SARs dealing with terrorism).

---

[8] Note that the bulk of this report was written prior to the Elmer rollout on 27 May 2005. In the event, as at end-June 2005 (when the report was finalised), it is far too early to gain an understanding of how the rollout is affecting LEA work.

[9] Eight LEAs (Avon and Somerset Constabulary, City of London Police, Her Majesty's Customs and Excise, Hertfordshire, Inland Revenue, Metropolitan Police Service, Scottish Drug Enforcement Agency, Thames Valley Police) piloted the remote Elmer system in a month-long test period beginning 24 February 2005. Rollout is scheduled to occur in late-May 2005. The piloting and rollout had originally been scheduled for autumn 2004, but were pushed back due to IT and legal issues.

LEAs will be entirely responsible for selecting the SARs they wish to view and work on. SARs will not have been searched against any external databases or Elmer itself for links to previous SARs (as LEAs will be able to do this themselves). LEAs wishing to search Elementary will need to lodge a search request with their regional NCIS office as per long-standing established Elementary search protocols. SARs will be available to print or download (though not yet in bulk); feedback will be provided online. NCIS states that it will continue to provide LEAs with various intelligence products and certain database queries.

- **Consent SARs are disseminated differently**. From March 2003-March 2004, all consents were disseminated to law enforcement for action. From March 2004 through to the present, if the consent SAR meets any of a number of criteria (e.g. property or subject leaving the UK; property is being converted to cash/equivalent, leaving the UK audit trail; the activity is fraud-related; the subject is flagged)—the consent is disseminated via fax to the appropriate LEA for action; if not, NCIS handles the consent in-house. Either way, NCIS conducts (and conducted prior to March 2004) various database checks prior to dissemination to LEAs or to the in-house approval/denial of consent. At present, NCIS handles roughly 65 percent of consents in-house, disseminating the remaining 35 percent to LEAs for action. Upon conclusion of the process (with consent being either granted or denied, or assumed if seven working days pass with no word), the consent SAR is input onto the Elmer database. The rollout of the Elmer database is not expected to affect consent procedures.

B. Scope of the Problem

7. But what happens to SARs once they are in the hands of LEAs? To what extent are SARs used by law enforcement? Do SARs play a role in the conviction of offenders and/or follow-on confiscations, or—despite the participation of the regulated sector—do they sit unused in office files or databases? In the event, very little is known about LEA use and management of SARs in the UK (and, indeed, in many countries). This is the motivation for the present study.

8. This is not to say that no sources discuss SARs and law enforcement. There are some general examples of LEA use of SARs (e.g. country-non-specific examples discussed in the FATF's annual typologies exercise, or the Egmont Group's 2000 *FIUs in Action* publication). Specific to the UK, passing mention is made of SARs in various *Money Laundering News* and *Proceeds of Crime Update* newsletters put out by the Assets Recovery Agency (ARA) and in the 2004 *Payback Time* report of Her Majesty's Inspectorate of Constabulary (HMIC). The Performance and Innovation Unit of the Cabinet Office (PIU) discusses the AML regime in detail in its influential 2000 *Recovering the Proceeds of Crime* report, though it focuses primarily on the roles of NCIS and the FSA. Occasional isolated internal reviews of the use and management of SARs by specific units have been carried out by a handful of LEAs (e.g. Dickin, 2001; Hicks, 2003).

9. The most comprehensive analyses of the use and management of SARs by LEAs are carried out by Gold and Levi (1994) and KPMG (2003). Gold and Levi (1994) present an examination of the SARs regime in the early 1990s (and their study raises many issues which remain salient today, including the problems being addressed by the present

research). Among other things, they look at a sample of 1,106 disclosures (referred to as FINLOGS at the time) to ascertain their contribution to criminal justice outcomes. Using a feedback/classification scheme previously employed by NCIS, they find that 1.4 percent of the sample were classified as "drug positive" or "crime positive" (i.e. involved an arrest); "this appears to be a poor total yield…", they comment.[10] They make a series of recommendations for financial institutions, NCIS, law enforcement, interagency communication and cooperation, regulators, and government. Most relevant to the present research: they recommend that the processes for the provision of feedback to the regulated entities are reviewed and potentially retooled; that NCIS becomes more proactive and successful in obtaining information on the progress of investigations; that forces should agree and develop a reasonably uniform policy with respect to acting upon and reporting back on disclosures; that more consideration should be given to protecting a certain amount of officer time from the intrusion of an excessive or uncontrolled amount of reactive work; and that government devotes sufficient funding to both reactive and proactive units to pursue disclosures.

10. KPMG (2003), the study widely credited with bringing about considerable recent change in the UK SARs regime, track a sample of 600 SARs from cradle-to-grave, in addition to other analyses.[11] They find that eleven percent of the 600 SARs contributed to a criminal justice outcome or were still being worked on; this represents some 34 percent of the 193 SARs in the sample for which outcomes were known. Further, KPMG makes 21 recommendations for improving the regime, seven of which are directed at LEAs. These include: the merging of financial investigation units on a regional basis (for smaller LEAs); the use of the ARA Centre of Excellence to develop guidance and training on use of SARs; LEA access to and use of Elmer terminals; the monitoring of LEA results and establishment of new service level agreements; the setting of LEA objectives by the Home Office which impact upon the use of SARs; the use of information available through Elmer to advertise successes of the regime; and the use of successes derived from the regime to support and assist resource allocation decisions.

11. But virtually no *systematic* information on LEA use (and management) of SARs is available for the UK. According to the PIU, "no records are kept of the quality of disclosures in the UK or the extent to which they have assisted law enforcement in prosecuting either money laundering or predicate offences" (PIU, 2000). Indeed, a large and growing list of commentators has highlighted the issue over the years, including Gold

[10] Gold and Levi also mention the categories of "drug suspect", "crime suspect", and "UNIDENT". The "suspect" categories refer to disclosures in which the subject was a suspect (likely identified in various database checks), while the latter refers to those cases "where officers feel instinctively that the transactions were linked to criminality but are a long way from even having evidence to satisfy themselves". The suspect categories represent 3.6 percent of the sample, while the UNIDENT represents 15.6 percent.

[11] As part of the 2003 report, KPMG also carried out an intensive survey of the users of SARs, including on several of the issues relevant to the present research. Specific survey findings were not published, and contributed only generally to the final KPMG report. KPMG very generously provided its survey data to the author of the present report.

and Levi (1994), PIU (2000), International Monetary Fund (2003), KPMG (2003), Transparency International (2003), Aldridge (2004), and HMIC (2004).[12]

12. A lack of systematic information on the use of SARs precludes any serious analysis of the efficacy of the AML regime in the UK and elsewhere. Admittedly, no perfect indicators exist which would allow for straightforward evaluation of the efficacy any AML regime. Reuter and Truman (2004) discuss various potential performance measures—but then note their associated and often crippling shortcomings; they do, however, get some mileage from "intermediate measures of performance such as the number of SARs, prosecutions, convictions and incarcerations, seizures, forfeitures". Recommendation 32 of the FATF's 40 Recommendations (2003 revision) calls for similar information:[13]

> Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR [SAR] received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation (FATF, 2003).

13. Further, the lack of systematic information on LEA use and management affects more than an inability to empirically analyse the efficacy of the regime. It also prevents the regulated sector from better targeting disclosures, and it chips away at the desire for industry to cooperate with reporting requirements. Both are critical. The imprecise targeting of disclosures implies that industry may not be finding the offenders or terrorists of most concern—and that industry resources are not being put to their most efficient use—while a loose targeting of disclosures (and perhaps an inappropriately low bar for suspicion) has the potential to swamp or at least clog the system with too many SARs. An uncooperative industry has the potential to effectively shut down the system (e.g. by lobbying Parliament for change in the legislation; by collectively refusing to disclose on various grounds, pushing the issue into the courts; or by intentionally employing the very lowest bar for suspicion—though doing so within the letter of the law—thus swamping the system).[14] Lastly, compliance officers/money laundering reporting officers need information to bring to their boards to justify AML expenditures.

---

[12] This lack of understanding does not appear to be exclusive to the UK. International experiences are discussed later in the present paper.

[13] The present research does not represent an empirical analysis of the efficacy of the regime. It is, however, a requisite step in that direction, exploring the current availability of intermediate measures, among other things.

[14] A number of sources share similar thoughts on the importance of feedback; see, for example, FATF, (2003), KPMG (2003), PIU (2000), FATF (1998), and Gold and Levi (1994). In particular, note Recommendation 25 of the FATF's 40 Recommendations:

> The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to

(continued)

C. Methodology

14. This research aimed to provide the kind of systematic information referred to above on the use and management of SARs in law enforcement agencies in the UK, to identify gaps in that information, and to propose actions to bridge such gaps. From the project's inception, it was decided that the research would represent neither an audit nor a "name-and-shame" of LEA performance on SARs.[15] The study was designed to suggest realisable improvements to the LEA share of a regime which draws from the direct participation of the private sector, NCIS, and law enforcement. In this regard, the study was intended to be of immediate use, and an ambitious time-frame of four months of active research was agreed (December 2004-March 2005, inclusive, with the write-up of findings in April-May 2005).

15. The study comprised four components, married together by a discussion-and-recommendations section:

- **Theoretical underpinnings**: It may be the case that industry/NCIS/LEAs expect too much of SARs (or, to be fair, perhaps too little), and/or that issues surrounding the understanding of the nature of SARs as information/intelligence fuel discontent. As such, this background component sought to examine what can realistically be expected of SARs, setting the stage for subsequent analysis.

- **UK LEA use and management of SARs**: This component represents the heart of the research. It included 1) a survey of the LEAs who deal with SARs; and 2) site visits with select LEAs. The survey of LEAs sought to gain a general understanding of nationwide use and management of SARs, as well as examples of their contribution to crime reduction and the availability of intermediate measures; site visits explored good practice in SARs management in the hopes that approaches could be replicated in LEAs around the country. Sites were selected for visitation on a number of criteria, including their size and location (urban v. rural) and on whether or not they were thought to employ sound or novel practice in the management of SARs (perhaps identified in the background research of the HMIC *Payback Time* report).

- **Overseas experiences**: This component of the research looked to select foreign jurisdictions for their experiences with reporting regimes. It sought to address questions including the following: have other jurisdictions faced similar concerns of industry—namely perceptions that little is being done with the reports provided, and/or that perhaps SARs (or similar reports) are of little crime-reduction value—and were such industry concerns appropriate; and what solutions were implemented by foreign jurisdictions to address such concerns.

---

combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions (FATF, 2003).

[15] LEAs were informed that the information they provided would be only presented in aggregate. Several tables in this report present information by LEA; this information has been provided by NCIS, and does not relate to LEA performance (but rather things like SARs allocations and disseminations).

- **Regulated sector desires for feedback**: This research is to some extent driven by the desires of industry for feedback on the use of information it provides. This component sought to clarify what sort of information the regulated sector was looking to receive.

16. The study drew extensively from 1) meetings and telephone/email conversations with a broad base of the SARs community from the private sector, government (including HO, HMT, FSA), and, of course, law enforcement (including NCIS); 2) the existing academic and policy literature; 3) conversations with relevant organisations in overseas jurisdictions; 4) site visits with select LEAs; and 5) a survey of LEAs. Opportunities for the validation of information provided and for follow-up with non-respondents were limited. To minimize the burden on an already survey-fatigued population of LEAs—and to avoid a wasteful duplication of effort—every effort was made to employ disparate but previously unreleased sources of information and to collaborate where possible (in this regard, the author received generous assistance from a number of individuals and organisations, including KMPG, NCIS, HMIC, and the FIWG; see the acknowledgements section for more information).

III. THEORY: SARS FROM INFORMATION TO INTELLIGENCE TO OUTCOMES

17. The theoretical support for AML regimes in general and for SARs in particular is covered by a number of existing sources. Most cite the ability of a SARs regime to deter and displace money laundering and predicate offences; to facilitate the detection and sanctioning of such crimes after the fact; and to disrupt such crimes in progress (see, for example, KPMG, 2003; Reuter and Truman, 2004; Gold and Levi, 1994; HMT, 2004).[17]

18. What is little discussed, however, is how SARs should work on a day-to-day basis to prevent criminal and terrorist activity, and—in particular—to sanction such activity after the fact. SARs are often discussed in the context of intelligence. The role of SARs as intelligence—or perhaps more accurately, as information which may or may not become intelligence, an important distinction—is often subtle. This section explores the journey from information to intelligence to outcomes; the section guides and informs subsequent analysis.

19. What is intelligence? There are few agreed-upon definitions of criminal and/or national security intelligence (a least in the public domain), though the point is clear enough.[18] Simply put, intelligence is "the considered and analysed product of systematic information gathering" (ACPO, 2001); "intelligence is evaluated information collected by various techniques for a defined purpose" (Higgins, 2004). Intelligence may be used for strategic and/or tactical (sometimes known as operational) purposes. Strategic intelligence refers to "an assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation"; tactical intelligence is "evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case" (Criminal Intelligence Training Coordination Strategy Working Group, 2004). In the UK, criminal intelligence (and increasingly policing) is guided by the National Intelligence Model (NIM). The NIM is a standardisation of strategic and tactical intelligence approaches and products.[19]

20. Are SARs themselves actually intelligence, whether tactical or strategic? As it happens, SARs *as received* are broadly *not* intelligence, not without further evaluation. The idea is as follows: "Upon discovering out-of-the-ordinary behaviour, the solver [i.e. intelligence analyst, crime analyst, investigator] looks for supporting data marking the observed signals as a true phenomenon and not just noise" (Hollywood *et al*, 2004). That

---

[17] To these are often added "to protect the integrity of the financial system" and "to avoid economic and competitive distortions" (HMT, 2004).

[18] For a discussion of the merits of various definitions of intelligence (including mention of the distinction between information and intelligence), see Warner (2002).

[19] The NIM divides criminality into three categories: *level one* for local issues; *level two* for cross-border issues; and *level three* for serious and organised crime (national and international). Policing and intelligence are guided by strategic and tactical *tasking and coordinating meetings*, all in support of the *control strategy* (which sets forth the intelligence, prevention, and enforcement priorities of the LEA). Four key intelligence products support strategic and tactical tasking and coordinating: *strategic assessments*, *tactical assessments*, *target profiles*, and *problem profiles*. For more information on the NIM, see, for example, NCIS (2000), Flood (2004), and Christopher (2004).

is, initial searches of existing sources of information, including various intelligence databases or Elmer itself (to check for links with other SARs)—coupled with the reason for suspicion—serve to filter out the noise, and to contextualise the information.[20] The process of evaluating "raw" SARs—through what are sometimes referred to as "initial checks"—is what transforms "suspicion-based information", as one NCIS staff member put it, into intelligence (and thus begins attrition).[21] The information evaluation does not necessarily need to be an involved process requiring considerable staff resources: the most efficient manner of at least some initial evaluation likely lies in the automated, electronic cross-checking of various databases (e.g. PNC) and, importantly, Elmer itself.[22] SARs evaluated to be indicative of truly suspicious behaviour may then be prioritised and further developed into usable intelligence. Intelligence development will generally entail deeper information cross-checking (from various sources of information) and analysis.

21. Investigation is distinct from information evaluation/intelligence development, though the line is a fuzzy one. By and large—and for the purposes of this paper—investigation implies evidence-gathering. Investigation will accordingly require the use of various court orders (e.g. production orders, search and seizure warrants) and perhaps operational or even specialist teams (e.g. surveillance teams, firearms teams). Operational teams may be required because 1) staff evaluating information and developing intelligence packages will not always have the proper accreditation to apply for court orders; and 2) the responsibility for intelligence development may have been separated from investigation, such that different parties carry out different functions within an LEA. Financial investigation unit (FIU) staff have historically been responsible for the receipt, evaluation, and development of SARs.[23] They have also been responsible for the investigation of proactive SARs-based cases which fall into the financial investigator (FI) remit, such as confiscation, money laundering. Proactive SARs-based jobs outside of FIU remits (e.g. operations relating to class A drugs), however, require assignment to operational teams for investigation through the tasking and coordinating process. Whether SARs-based cases

---

[20] This is not to suggest that the information-to-intelligence process works perfectly: in cross-checking SARs, a certain percentage will be wrongly dismissed as useless information (i.e. false negatives), destined not in the near-term to become actionable intelligence; some which should have been dismissed will clear the hurdle to intelligence (false positives). As SARs sit on Elmer, however, even SARs which appear useless in the near-term may at some point suggest criminal behaviour, perhaps when linked to several other SARs over the course of several years.

[21] There may be disagreement over the wording here: as received, SARs may be considered by some to be intelligence (in fact, SARs may or may not be classified as intelligence simply for policy reasons: items classified as intelligence must be handled and distributed according to certain guidelines). The critical point does not, however, depend on semantics: if SARs as received are *information*, then they need to be somehow evaluated and to become *intelligence*; if they are considered *intelligence* as received, they still need to undergo the same evaluation/development that turns them from intelligence to *actionable intelligence.*

[22] KPMG (2003) encouraged NCIS to carry out automated searches of Elmer, PNC, Cedric, and Alert for the prioritisation of SARs to LEAs. Thus far, there is no facility at NCIS to allow for such automated database checks.

[23] Note that the acronym FIU refers in the present report to a financial *investigation* unit, as opposed to a financial *intelligence* unit; the latter typically refers to the national-level organisation within a jurisdiction which receives, analyses, and disseminates SARs (and potentially threshold-based reports). NCIS is the national financial *intelligence* unit of the UK.

are actually assigned to operational teams will depend on the power of the intelligence, the availability of operational resources, and the current priorities of the LEA.

22. Should the simple *receipt* of SARs by NCIS/LEAs then consistently lead *directly* to *full-on investigations and arrests*? The simple answer appears to be no, with important caveats.[24] This is for two related reasons. First, as noted above, SARs must be turned from information to intelligence (either by NCIS or LEAs, automatically or manually) prior to launching investigations. This weeding out (though not deleting) of noise is important not least because defensive reporting or mistaken suspicion on the part of filers may lead to a virtual mountain of information, some of which may be of limited value.[25] Second, law enforcement in the UK, as elsewhere, operates in a resource-constrained environment.[26] The deployment of investigative operational teams to fully investigate each and every SAR as received is almost certainly not the best use of limited resources.[27] This is the case not least because SARs may become useful as they accumulate (one SAR may or may not suggest true criminality, but multiple SARs over time may indeed suggest an ongoing course of crime with one or more offenders—calling for law enforcement attention). That is, in an environment of limited resources, unless a SAR clearly indicates serious criminality, it may be difficult for managers to approve the deployment of teams who may require costly surveillance support (and who will most certainly need to spend time in court obtaining production orders and the like) on the basis of a single SAR which represents nothing more than suspicion (Gold and Levi (1994) come to similar conclusions).

23. But herein lie the important caveats: SARs will in some cases clearly suggest the most serious of criminality, and (and/or) require little if any further intelligence development or law enforcement investigation. Even in a resource-constrained environment—or perhaps particularly in a resource-constrained environment—it would seem foolish to ignore such "hot" intelligence. In other words, while it may be the case that relatively few should be directly actioned, it seems wrong on the face of it to dismiss the potential for SARs' direct contribution. It is important that mechanisms are in place to

---

[24] This section discusses SARs in general; consent SARs may in fact lead more directly to certain outcomes than their nonconsent brethren, not least because of the need for timely action by NCIS/LEAs.

[25] *Defensive reporting* may be defined as the reporting by industry of each and every transaction with even the barest hint of suspicion. While defensive reporting is within the letter of the law (indeed, the practice exists to comply with the law), it very likely leads to false positives. The possibility remains that there may even be instances of what could be called offensive reporting, disclosures of activity in effort to deceive and/or clog the system. Also, the Bichard Inquiry flagged up misunderstandings surrounding the concept of "weeding out" of seemingly useless information/intelligence (Bichard, 2004). In the present report, weeding out implies the separating of wheat from chaff, though not the permanent deleting of the chaff.

[26] That law enforcement operates with constrained resources is one of the drivers behind the intelligence-led policing movement (see, for example, the demand gap discussed by Flood, 2004).

[27] In fact, it is also the case that it is likely inefficient to fully investigate each and every SAR which is defined as actionable intelligence; some activity, while illegal, may simply not be worrisome enough to warrant the use of scarce policing resources (more formally, the marginal cost of prevention/enforcement for the crime in question may be greater than the marginal benefit of preventing/enforcing the law with regard to that particular crime, bearing in mind that there are very likely dynamic aspects to the scenario).

identify such SARs (or trends in SARs which together indicate criminality).[28] Moreover, while the simple receipt of SARs may not on balance consistently lead directly to investigations, receipt should consistently lead to the kind of information evaluation—by NCIS or LEAs or perhaps both (with different sources of information), perhaps electronically—which separates wheat from chaff, potentially generating intelligence to be used for new and existing investigations.[29] Also, many SARs relate to targets of existing law enforcement operations or confiscations. Their receipt will not then lead to new investigations, but may directly play a crucial role in assisting existing ones with new information. Finally, the use of SARs in guiding the investigation and possible arrest/conviction of offenders is a tactical use; SARs may also be employed strategically, with less visible and less immediate outcomes.

24. Some limited disagreement exists on maximising the benefit of SARs. There are occasional suggestions that SARs should *not* all be examined/evaluated upon receipt (by either NCIS or LEAs); rather, the appropriate use of the data is in the interrogation of the database itself with specific queries (e.g. *have SARs been made against this target?* or *who are the most prolific money launderers?*). This suggests that the two methods—evaluate SARs as received v. interrogate the database—are mutually exclusive, which they're not. It seems logical that both methods should be employed: to ignore the former is to ignore the potential for SARs to indicate intelligence on previously unknown criminal/terrorist activity, which may be imminent; to ignore the latter is to assume that critically important patterns will be apparent as and when SARS are received, which they likely won't. This is not to say that SARs as received must be *fully investigated* one-by-one (on the contrary, as noted above), but rather that they should at least undergo some sort of prompt initial evaluation (perhaps electronically, with keywords or various data-mining techniques, many of which could be automated) to capture the hot intelligence and to assist in workload prioritisation, in addition to database interrogation.[30]

25. Once intelligence, however, SARs can and in many cases should lead directly to proactive investigations or should contribute to ongoing investigations, all with various criminal justice outcomes. In this regard, there are a number of tactical and strategic uses to which SARs may be put. Perhaps the most critical point to bear in mind is that the all-crimes nature of the legislation implies that the regime is designed to be used in the prevention and enforcement of a far wider range of crimes than financial crime and money laundering alone. SARs may be useful in identifying the criminality, assets, or methods of a burglar or car thief just as much as drug dealer, VAT fraudster, or, indeed, stereotypical money launderer (and it may be the case that the personal details, like telephone numbers and addresses, are more important to law enforcement officers than the suspicious activity itself). Tactical and strategic uses of SARs are presented in Table 1.

---

[28] Gold and Levi (1994) suggested that reporting entities highlight those activities/transactions which seem highly likely to be suggestive of money laundering (in contrast to the current approach of limited value intelligence reports).

[29] The rollout of Elmer will put the onus largely on LEAs in the tactical intelligence development arena.

[30] Notes NCIS: "the law enforcement environment is, however, a fast moving one in which matters requiring urgent attention are frequently likely to come to notice. Whilst it remains essential that the sense of direction be maintained, a fast track procedure for actioning urgent intelligence is necessary" (NCIS, 2000).

Table 1. Uses of SARs in an Intelligence Context

Use type	*Use*
Tactical	To identify previously unknown criminal(s)/terrorist(s)
	To identify the previously unknown criminal/terrorist activity of a known criminal/terrorist
	To corroborate known criminal/terrorist activity
	To identify criminal/terrorist networks
	To enhance existing criminal/terrorist investigations (e.g. with new avenues for investigation)
	To identify/locate assets for cash seizure/forfeiture, restraint/confiscation, and/or Hansard valuation (on unpaid tax, carried out by Inland Revenue)
	To assist in confiscation order enforcement (and, potentially, fine enforcement)
	To prevent dissipation of assets and/or to disrupt current criminality/terrorist funding (e.g. through consent SARs)
	To identify patterns of high- or low-volume reporting for regulated entity self-assessment or regulatory/LEA follow-up
	To identify the potential duplicity of regulated entities
Strategic	To contribute to strategic assessments (e.g. for the annual *UK Threat Assessment* exercise)
	To identify the main threats, risks, patterns, and emerging trends in money laundering/financial crime, including identifying typologies to provide better understanding of the problem
	To satisfy international commitments

Sources: Various, including MLRTF (2004a), FinCEN (1999), Levi (1996).

26. Intelligence is typically discussed in the context of an intelligence cycle (see, for example, CIA, 2002; Ratcliffe, 2004), whose steps, in order, include planning, collection, processing, analysis, and dissemination. What makes the process a cycle is the feedback loop that links the last phase, dissemination, to the next planning phase. With intelligence derived from SARs, as with other intelligence, it is critical that this loop is closed with feedback from the consumer of the intelligence to the decision-makers in planning and collection. That is, the LEA users of SARs should provide feedback on the value of the SARs-based intelligence; the uses to which it was put, such as those described above; and its impact on crime-reduction. This feedback (the feedback suggested by the FATF in its recommendation 32, discussed above) should be provided to NCIS and ultimately to industry (sanitised). It should allow for better (i.e. more precise, more meaningful, and perhaps as a result, fewer) SARs in future disclosures. Feedback should be given by LEAs to NCIS whenever SARs are examined, even when a SAR seems unrelated to crime. This may allow for better industry targeting of truly suspicious behaviour. Feedback is a powerful tool for improving the efficiency of the regime in its entirety.

27. It would be wrong to assume that the provision of feedback is straightforward, however. First of all, truly meaningful feedback may require the input of a number of people, including the initial users of SARs (in information evaluation/intelligence development), any investigative teams, and potentially the CPS/courts. It may be the case that whilst initial SARs users were positive on the importance of SARs (perhaps in identifying a previously unknown criminal), the resulting case was difficult to sell to operational teams (perhaps because other priorities were facing the LEA at the time, driving the control strategy in a different direction). While a consent SAR may quickly and directly lead to an outcome like cash seizure, this is probably the exception not the norm. Considerable time may pass between the initial viewing of a SAR and the final outcomes of conviction/confiscation. Complex excise cases (e.g. VAT fraud, MTIC

fraud) can take years simply to get to court, let alone run their course.[31] By that time, the users of the relevant SARs, if SARs were responsible early on for initiating the investigation, may have moved on to new positions, or may have left the LEA entirely. Even those SARs initially assessed as unconnected to crime may turn out months or years later to link to other SARs, suggesting a hitherto unseen course of criminality—and requiring new feedback. Human nature may be relevant as well: investigators may wish to take the credit for successful operations, when ultimately it was the intelligence that saved the day. Lastly, while feedback should not be time-consuming (once policies and procedures are ironed out, the actual feedback itself may require only minutes or even seconds), comments received in this research suggest a perception on the part of LEAs that time spent providing feedback is time diverted from actual crime-fighting. This is not the case, though LEAs may need to be given certain feedback incentives to compensate for this belief.

28. Finally, interpreting and analysing the feedback, particularly in gauging the efficacy of the regime, is itself complicated. The FATF and others all rightly call for some feedback/intermediate measures of the use of SARs. After all, such measures (which are based primarily on an understanding of how LEAs use SARs, most efficiently won through some sort of feedback mechanism), are critical for understanding the contribution that an AML regime makes to the reduction of crime/terrorism. But this doesn't imply that such measures are easily understood.[32] Uses of SARs are not mutually exclusive: one or many SARs, for example, may indicate unknown criminality *and* prevent dissipation of assets for the same offender. Or many SARs together will be used to illustrate the pattern of offending of a lone individual. As an example, assume that the regulated sector files 100 SARs in a year. Feedback may suggest that these 100 result in one conviction, but it may be the case that 10 or even 50 of the SARs played a role in that conviction. It might be misleading, then, to look at the number of convictions resulting from SARs (one conviction secured as the result of 100 SARs filed), though perhaps less misleading to look at the number of SARs which contributed to a conviction (10 percent of the 100 SARs filed contributed to a conviction).[33] Of course, many SARs will be received relating to people already under investigation; an indicator such as SARs launching proactive investigations must then look at SARs launching proactive investigations as a percentage of SARs received relating to people not already under investigation, not all SARs received. And what is the basis for performance assessment? Is the hypothetical 10-percent-of-the-100-SARs-filed example indicative of a successful regime, or one in need

[31] Along these lines, note that the Inland Revenue use of SARs is naturally historic: SARs are of less importance to investigations unless the relevant tax forms have been returned to IR.

[32] This is also pointed out by the MLRTF in its Second Report to Ministers. HMIC (2004) suggests that simple measures like the percentage of SARs leading to investigations are misleading, though no specific alternatives are offered.

[33] Timing is also a complicating factor: because no immediate investigation/conviction doesn't imply that no investigation/conviction will ever take place, it might be most appropriate to consider the number of SARs contributing to a conviction as a percentage of the SARs filed in the previous year (or even the year before that), not least because the number of SARs filed per annum has been increasing. Finally, the interpretation of feedback on SARs contributing to convictions should be mindful of the fact that once in the courts, cases may fail due to outside factors unrelated to SARs (the same goes for prosecutions, confiscations, and the like).

of work? Should such feedback be interpreted as indicative of the failure of SARs to reduce crime, or of limitations in the functioning of the regime itself (e.g. SARs when disseminated were too old to be of significant use)?[34] Lastly, feedback and intermediate measures suffer from one inescapable but crucial weakness: they cannot capture the unknowable counterfactual (i.e. what would have happened in the absence of the regime). SARs most certainly deter money laundering and predicate criminality/terrorism—but the level of deterrence is very difficult to determine empirically.

29. What are the implications for the regime and the research? All of the above is simply to suggest *not* that indicators are fatally flawed, but that interpretations of statistics on the use of SARs are proxies for the truth, and must be mindful of the details of what is being measured. This should be considered later in the present paper when interpreting findings. Moreover, knowing what can reasonably be expected of SARs from information to intelligence to outcomes helps to analyse what is done in practice.

[34] Gold and Levi (1994) usefully differentiate between implementation failure and theory failure.

IV. FINDINGS

30. This chapter presents the results of the research, beginning with experiences in the UK, moving to experiences in overseas jurisdictions, and followed by findings related to the regulated sector and its desires for feedback. SARs-related case examples are presented in an appendix.

A. UK LEA Use and Management of SARs

31. So how do law enforcement agencies in the UK use and manage SARs? Do SARs appear under-utilised? How adequate are LEA statistics on use? Is feedback ever given? While recognising that the sections to some extent overlap, findings specific to the UK are presented in sections on the users of SARs; management of SARs (processes); uses of SARs (outcomes); feedback to NCIS/industry; and the system in flux. Information is drawn from a survey of LEAs; formal site visits with select LEAs; discussions with a broad swath of the LEA SARs community; and data provided by NCIS, HMIC, and KPMG. For the survey of LEAs, responses were received from 49 of the 50 LEAs in the primary SARs user community (NTFIU declined to respond to the survey for security reasons, so it would be fair to say that the response rate was 100 percent). Site visits were carried out with City of London Police, Devon & Cornwall Constabulary, Her Majesty's Customs and Excise, Inland Revenue, Metropolitan Police Service, National Crime Squad, Norfolk Constabulary, NTFIU, Scottish Drug Enforcement Agency (informed also by a visit with Strathclyde Police), and West Midlands Police.

32. Much of the information below is, of course, historical in nature. The system continues to change, and the rollout of the Elmer database to LEAs nationwide may indeed represent a tectonic shift in the LEA approach to SARs. That the system is changing is not, however, a sufficient reason to postpone or ignore the research—not least because the regime has been in flux for years. There will always be some considerable change just around the corner, like the Elmer rollout or the launch of the new Serious Organised Crime Agency (SOCA); waiting for the perfect time to conduct the research would be fruitless. Moreover, the regulated sector and policy makers have a right to know how and to what extent SARs are being used (information that will be historical in its very nature). Without such periodic reflective analyses, there is no way to learn from past mistakes and successes.

33. A note on statistics: inconsistencies have been identified in statistics provided by LEAs and by NCIS, which are used throughout this report. Inconsistencies are both internal (between different statistical representations of the same concept), and external (between statistics provided and numbers reported in previous recent reports). Inconsistencies are generally minor, but are indicative of limited quality control.[35]

[35] An LEA-related example: for several LEAs, the number of consents granted plus consents refused does not add up to the number of consents received. An NCIS-related example: KPMG (2003) notes that 63,000 SARs were received by NCIS in 2002; statistics provided for this initiative suggest that some 56,000 were received. NCIS states that the difference is explained by the inclusion of search requests and requests from overseas national financial intelligence units in the numbers provided to KPMG (the 56,000 represent strictly new SARs filed by the regulated sector, according to NCIS).

1. Users of SARs

34. The LEA SAR user community is broad. It comprises 50 primary user organisations: the 43 territorial police forces of England and Wales; the Police Service of Northern Ireland (PSNI); the Scottish Drug Enforcement Agency (SDEA), which since end-2002 has been the SARs conduit for the eight Scottish territorial police forces and the SDEA itself; and a number of national LEAs, including the Department of Work and Pensions (DWP), Her Majesty's Customs and Excise (HMCE), Inland Revenue (IR), National Crime Squad (NCS), and the National Terrorist Financial Investigation Unit (NTFIU). This research will focus on 49 primary users; much NTFIU use and management information is too sensitive for publication.[36] For completeness, note that the Assets Recovery Agency (ARA) employs SARs in its work, though generally by requesting them from NCIS. The Financial Services Authority (FSA) occasionally receives SARs relating to regulatory matters. NCIS itself is also a user of SARs: NCIS divisions may utilize SARs in other NCIS work (e.g. on drug trafficking), and the NCIS SFI uses SARs in tactical and strategic intelligence product development. Primary users are presented in Table 2, which illustrates SARs allocated and disseminated to the 49 LEAs in 2003 and 2004.[37]

[36] Very little information on the work of the NTFIU is available in the public domain, though see HMT (2002).

[37] SARs are occasionally sent to the law enforcement or equivalent sections of a number of other organisations, including the British Transport Police, Department of Trade and Industry, Ministry of Defence Police, and the Serious Fraud Office. The five Regional Asset Recovery Teams set up in England and Wales in 2003 and 2004 employ SARs through search requests, but do not otherwise actively receive SARs from NCIS. These organisations were not included in the research proper. SARs may also be sent to national financial intelligence units in foreign jurisdictions, usually at their behest.

Table 2. Primary Users of SARs (with 2003-2004 Annual Allocations and Disseminations)

	2003		*2004*	
LEA	***Allocations***	***Total disseminations***	***Allocations***	***Total disseminations***
Avon & Somerset Constabulary	1,337	527	1,867	204
Bedfordshire Police	866	280	1,389	120
Cambridgeshire Constabulary	735	303	1,159	165
Cheshire Constabulary	713	236	1,279	158
City of London Police	503	366	695	269
Cleveland Police	399	204	595	77
Cumbria Constabulary	317	165	392	82
Derbyshire Constabulary	706	324	1,043	110
Devon & Cornwall Constabulary	971	439	1,597	161
Dorset Police	700	294	1,202	100
Durham Constabulary	376	151	510	90
DWP	330	103	889	1,147
Dyfed Powys Police	328	93	650	73
Essex Police	1,502	568	2,145	237
Gloucestershire Constabulary	403	232	582	78
Greater Manchester Police	3,078	1,070	5,050	520
Gwent Police	330	105	586	64
Hampshire Constabulary	1,508	505	2,156	195
Hertfordshire Constabulary	1,106	455	1,632	138
HMCE	13,357	28,663	6,398	10,573
Humberside Police	604	267	968	99
Inland Revenue	5,406	4,127	9,126	9,662
Kent Police	1,413	713	2,042	276
Lancashire Constabulary	1,658	599	2,756	302
Leicestershire Constabulary	1,136	579	1,681	203
Lincolnshire Police	363	162	643	124
Merseyside Police	1,154	1,003	1,789	260
Metropolitan Police Service	27,093	11,229	39,150	3,846
NCS	443	498	372	379
Norfolk Constabulary	586	231	925	131
North Wales Police	381	107	680	55
North Yorkshire Police	372	188	627	115
Northamptonshire Police	556	231	844	88
Northumbria Police	1,096	437	1,545	150
Nottinghamshire Police	1,057	441	1,519	145
PSNI	3,210	1,070	4,125	1,473
SDEA	3,369	2,216	4,472	751
South Wales Police	912	619	1,311	174
South Yorkshire Police	1,223	592	1,809	244
Staffordshire Police	829	296	1,287	159
Suffolk Constabulary	578	203	732	90
Surrey Police	2,068	550	3,151	263
Sussex Police	1,526	546	2,223	223
Thames Valley Police	2,843	983	4,666	326
Warwickshire Police	336	114	548	51
West Mercia Constabulary	1,017	293	1,653	185
West Midlands Police	3,862	1,595	5,985	666
West Yorkshire Police	2,489	951	3,709	398
Wiltshire Constabulary	532	175	979	70

Source: NCIS. Total disseminations include LEA-bound consents and SARs which have been copied to more than one LEA (this explains why HMCE, for example, has more SARs disseminated than were originally allocated). Total disseminations exclude SARs related to terrorism and various other sensitive issues; SARs destined for overseas jurisdictions; SARs sent out in bulk backlog-clearing exercises (see footnote 44); and SARs sent to NCIS units other than SFI. NTFIU allocations and disseminations are classified. SARs may also be allocated and disseminated to certain specialised users, who are not presented here. NCIS SFI is also a user of SARs. SARs are occasionally disseminated directly to various Scottish forces (as a result of specific search requests or flagged targets); these have been included with the SDEA figures.

35. **Unit types**: Units which deal with SARs vary in size and composition. Three models prevail: 1) the FIU with shared SARs responsibility; 2) the ring-fenced SARs development unit within an FIU; 3) and the financial intelligence development unit (FIDU). FIUs are the traditional users of SARs.[38] The *FIU with shared SARs responsibility* refers to the FIU found in many police forces which deals with all things POCA, including cash seizure, confiscation, and SARs. All staff deal with SARs as and when they can. Because SARs work is not protected, however, other FIU priorities (e.g. confiscations, cash seizures) may overwhelm the time available for SARs development. The upside of the shared-responsibility approach is that staff evaluating/developing SARs can and do also carry out the investigation of certain SARs packages. The second approach, the *ring-fenced SARs development unit* model, refers to what is a subunit of the FIU with a specific remit to deal with SARs (and financial intelligence development). SARs development may be handled by one FI (often a retired police officer rehired as a civilian accredited FI) or sometimes a researcher or clerk or indeed sometimes a team thereof. The benefit of this type of unit is that resources are fully devoted to evaluating and subsequently developing SARs into intelligence packages for use by the wider FIU or to be sent to tasking and coordinating to become full-blown investigations. The workload of this unit-within-a-unit model typically is restricted only to information evaluation/intelligence development; no investigation is carried out. Despite the name, staff are not always ring-fenced, and may occasionally be called to perform other duties, but the concept is one of a separation of responsibilities. The last model is the *FIDU*, which is responsible solely for evaluating information and developing intelligence packages (not investigating), like the ring-fenced model, but is larger—and independent of the FIU. FIDUs are typically found in larger LEAs, like the MPS and SDEA. FIDU work is to some extent more analytically advanced than with the smaller ring-fenced model. Not surprisingly, there is some limited evidence which suggests that the FIDU/ring-fenced models are more efficient than the shared-responsibility model, as SARs cannot simply fall through the cracks (Hicks, 2003). Twenty-eight LEAs appear to employ the shared-responsibility model; 18 LEAs use the ring-fenced approach; and three LEAs have FIDUs.

36. **Resource levels**: The 49 LEAs were asked about the overall levels of full-time equivalent (FTE) staffing of their units, and the number of FTE staff dedicated to SARs duties (i.e. evaluation/development, not investigation, which will happen with a wider community of staff LEA-wide). LEAs identified a total of 520.5 overall FTE staff, of which 80 were dedicated to SARs. The overall figure is a lower-bound estimate of the number of overall staff, as two LEAs provided no information in this regard (one of which is a national organisation with at least 50 relevant staff); several LEAs also have staff in the field (outside of headquarters units or, in the case of the SDEA, in the Scottish territorial forces) who will perform relevant duties. Similarly, the latter figure on SARs-dedicated staff is itself an underestimate. As noted above, most LEAs employ the shared-responsibility approach to dealing with SARs. Sadly, no indication was given concerning

[38] Several police LEAs have Economic Crime Units, which for all intents and purposes resemble FIUs (these Economic Crime Units may house FIUs and Fraud Squads). For the purposes of this paper, Economic Crime Units will be considered as FIUs. Also, for two national LEAs, SARs are initially sent to a central unit simply as a point of receipt, from which SARs are sent to FIUs in the appropriate regional offices for evaluation/development/investigation. These organisations have been classified as using the *FIU with shared SARs responsibility* model.

the percentage of overall staff dedicated to SARs-related activities. Assuming 15 percent of work-time is dedicated to SARs in these units (as does KMPG (2003), guided by HMCE), this implies that the total level of SARs-dedicated staff is 119 nationwide (80 from above + 39 from the shared-responsibility units).[39] Assuming 25 percent of work-time is dedicated to SARs (which may have been the case prior to the June 2004 slowdown of nonconsent dissemination), this implies that the total level of SARs-dedicated staff nationwide is 145. All of this is relatively consistent with KPMG (2003), which identified some 500 overall staff and 157 SARs-dedicated staff nationwide.

37. That said, ARA maintains statistics on the number of course attendees for its courses (though it has no firm count of the number of FIs performing FI duties, as some may have been trained but then relocated to other tasks). As at December 2004, these included 762 for the initial FI course; 348 for the confiscation course; and 151 for the money laundering course. Undoubtedly there is overlap between the attendees, but this is certainly suggestive of at least 762 FIs nationwide, a good number of whom will deal with SARs. Further, NCIS has trained approximately 250 LEA personnel on use of the Elmer database to support the rollout. Many of these 250 also hold the responsibility of further training personnel back in their LEAs, suggesting that the these estimates of FTE SARs-dedicated personnel may be low

38. Resource levels remain little changed since 2002 (10 LEAs identified SARs-specific increases of 19 staff—though eight LEAs provided no information in this regard). This is particularly disappointing considering the 176 percent growth in SARs reporting by the regulated sector between 2002 and 2004 (though there was little associated growth in dissemination from NCIS). In the event, a small number of LEAs hired staff in 2004 specifically to deal with SARs. Because NCIS significantly reduced the dissemination of nonconsent SARs in June 2004 (with no consultation with LEAs), some of these new staff were subsequently pulled to other duties.[40] These few LEAs hope that they will be able to pull the new staff back to SARs-related work when Elmer is rolled out. Many LEAs noted that they intend in the future to hire new personnel to deal with Elmer, who are not included here.

39. **FIB v. FIU**: Lastly, an ACPO position has emerged from the ACPO Proceeds of Crime Working Group concerning the responsibility for SARs and the Elmer database when rolled out to police forces (this is not relevant for non-police agencies, of course). Though the policy appears not to be set in stone, forces are encouraged to give much responsibility on SARs, through Elmer, to force intelligence bureaux (FIBs). The idea is that SARs will be mainstreamed by giving Elmer to FIBs, who should have a finger on the broader pulse of criminality in the area than FIUs—and who may thus make broader use of SARs. An informal survey of FIBs conducted on behalf of the author by the ACPO Lead on Intelligence Issues suggests that FIBs are not necessarily opposed to the concept, though with certain caveats. FIBs did feel that access to Elmer would be of use. But FIBs didn't seem to want sole responsibility for SARs (comments suggested that resource

[39] Gold and Levi (1994) also suggest that FIs spend roughly 15 percent of their time on SARs.

[40] These few LEAs could have tasked new staff to more proactively/aggressively engage with NCIS on SARs-related work; it's unclear why this didn't happen.

constraints would prevent FIBs from evaluating SARs upon receipt).[41] So if both FIBs and FIUs will be dealing with SARs, it is critical that steps are taken to prevent any duplication of effort. Conversations with the current police users of SARs suggest opposition to the FIB policy. This is likely in part due to a parochial desire to protect FIU turf—but certain issues deserve consideration. There seems to be some fear that broadening the user base to FIBs might be a threat to quality control: will FIB personnel recognise the often complex varieties of financial crime (like certain frauds)? More importantly, there is a worry that FIB personnel won't follow through on the critical issues surrounding the confidentiality of SARs (including consistent application for Public Interest Immunity). And most FIUs already coordinate to some extent with FIBs: more than 90 percent of the LEAs appear to log some or all SARs received on force intelligence systems. While an excellent step toward the mainstreaming of SARs/Elmer, the FIB policy needs further consideration/modification with input from both FIs and intelligence officers.

2. Management of SARs (Processes)

40. What, then, happens to SARs upon receipt by the LEAs? As noted in Chapter III, SARs may be evaluated upon receipt (and subsequently developed/investigated if appropriate); SARs may also be subjected to deeper interrogation/analysis of the *who are the most prolific offenders* sort. On the former—which seems to be the approach employed by most LEAs—SARs are dealt with in three main stages: information evaluation, intelligence development, and investigation (see pages 13-17 for background information on the progression of SARs from information to intelligence to outcomes; note that the three stages are an heuristic device of the author, and are not necessarily referred to by name by LEAs in their daily work). Not surprisingly, workflow is fairly uniform across LEAs, though the depth of work varies, as does the percentage of SARs subject to various stages of the process. The nonconsent process is described first, followed by consents.

41. **Nonconsent process**: Upon receipt, SARs are typically logged onto the unit's internal database and thus begins information evaluation. The information evaluation stage is used to separate wheat from chaff. This is done through basic database checks and a reading of the SAR itself (particularly the reason for suspicion). The majority (nearly 75 percent) of the LEAs reported that all SARs received undergo initial database checks. Databases checked commonly include PNC and other national sources of information (e.g. Companies House, Land Registry) as well as local intelligence systems, including that of the unit itself (with previously received SARs).[42] LEAs stated that SARs received on known nominals, relating to ongoing investigations, or with other positive database hits are generally progressed to intelligence development. SARs without any hits are typically retained for intelligence only (feedback will often be sent to NCIS at this point).[43] A few

[41] And FIBs would presumably have no interest in becoming involved with the consent process.

[42] National LEAs—particularly HMCE and Inland Revenue—appear to have broader sources of information at their disposal.

[43] SARs retained for intelligence only include SARs received with no apparent suspicion.

LEAs specifically noted that the text of the SARs themselves would be sufficient to generate further activity. Several LEAs reported that they simply did not have the resources to give SARs much more than a cursory read, if that—let alone carry out database checks. Similarly, a few others noted that everything was dependent on the daily workload: a heavy workload on the day of receipt implied few SARs were evaluated (this seemed to be the norm for these LEAs). Those LEAs who don't subject SARs to *any* initial checks (evaluation) will clearly miss SARs received on current targets (i.e. subjects of ongoing investigations) and perhaps imminent criminal activity. The rollout of Elmer will have implications for information evaluation; this is discussed is greater detail below (see page 46). In short, LEAs will need to find methods of evaluating SARs which don't command undue levels of resources; Phase II of the Elmer rollout will likely go some way to alleviating resource issues with advanced analytical capabilities.

42. The SARs which through information evaluation warrant further work are developed into intelligence packages. The intelligence development stage of the process includes firmer identification of SAR subjects and associates, banks accounts, assets held, and the source of funds (and analysis thereof). Reporting institutions are usually contacted (or may have been contacted in information evaluation, above). Any SARs relating to ongoing investigations are typically forwarded to the relevant unit within the LEA. LEAs noted that priority is often given in this stage to developing packages relating to current performance indicators, mostly confiscations and cash seizures, or larger force/national priorities. A small number of LEAs reported using systems/checklists/matrices to prioritise those SARs for evaluation/intelligence development based on set criteria. Such prioritisation systems will presumably be a necessity with the rollout of Elmer.

43. Intelligence development ends at the need for evidence gathering—where investigation begins—through various court orders and the like. Intelligence packages which require proactive investigation are sent to NIM tasking and coordinating for potential assignment to operational teams (surveillance teams, serious and organised crime teams, drugs teams, etc.). Intelligence packages for money laundering teams—packages put together by these same teams—seem to be handled in the FIU without going to the broader tasking and coordinating forum. SARs-based work vies for resources with other work brought to tasking and coordinating. The majority of LEAs suggested that less than ten percent of jobs (i.e. cases) in their units based on SARs required allocation to operational teams/outside units. This seems low; there are some indications that the question was understood to read what percentage of jobs are *actually assigned* to (i.e. taken on by) operational teams, not what percent would *need* operational assistance.

44. **Consent process**: The consent process is slightly different. NCIS will have carried out some initial checks on national databases by the time a consent is sent to LEAs; the LEAs will typically run local database checks (e.g. local force intelligence databases). Consent with then be either granted or denied, depending on the results of checks. In some cases, consent will be granted to tee off a proactive cash seizure. Most LEAs (nearly 85 percent of the 49) reported that they prioritise consents over nonconsents, and LEAs appear to believe that consents must *all* be acted upon. This is in contrast to recent comments received by NCIS which suggest that LEAs have the choice to work on consents or not; they can either give immediate consent or let seven working days pass with no action (in which case consent is assumed). The choice would fall with the LEA, presumably driven by resource constraints. And on resource constraints: LEAs were

asked what percentage of the unit's resources were consumed dealing with consents. Nearly 90 percent of the 49 LEAs stated that consents consume 20 percent or less of the unit's resources. Of course, many LEAs will have considerable amounts of other work to do (particularly those units employing the *FIU with shared SARs responsibility* model), so this percentage may be sufficiently high to be disruptive. This number may be less meaningful given the June 2004 reduction in nonconsent SARs, as LEAs may have more available time to action consents.

45. **Interrogating the information/intelligence**: One thing is to evaluate/develop SARs as received; another is to interrogate the information/intelligence. In the absence of access to Elmer (i.e. prior to rollout), interrogation occurs by turning to internal LEA databases which house information on those SARs disseminated by NCIS to the LEA and/or by sending search requests to NCIS to search Elmer in its entirety. And two main types of interrogation exist: 1) questions on known targets, like *does this current operational target have any SARs filed against him/her?*; and 2) questions which let the data speak for themselves, like *who is the most-disclosed upon individual in the boundaries of the LEA?*. LEAs were asked the following question: *for those investigations which have not been launched by the receipt of one or more SARs, do you ever turn to SARs (i.e. your SARs database or files, or force intelligence if SARs are loaded there) as a source of information/intelligence?* Nearly 90 percent of LEAs reported that they would turn to SARs in this manner. But there was only limited evidence of LEAs using SARs for advanced analytical work, and very few LEAs appear to interrogate SARs with the *who is the most-disclosed upon* type of questions. LEAs do not yet seem to have tuned in to this analytical approach. On search requests: the 49 LEAs filed 1,418 search requests in 2003 and 2,210 in 2004, for a total of 3,628 search requests filed in the two years together (the vast majority of which were filed by HMCE, Inland Revenue, and the MPS). It is difficult to say if this represents an under- or over-reliance on the search request mechanism. There was a noticeable increase of search requests filed as a percentage of SARs disseminated to the 49 LEAs beginning in June of 2004, at which point NCIS reduced the number of nonconsent SARs disseminated for action. Interestingly, this seems to be the result of a decrease in disseminations, not an increase in search requests (one would have imagined an increase in search requests to compensate for the reduction in disseminated nonconsent SARs). A number of LEAs suggested that because the search request process was laborious and too time-consuming, it was little-used. Clearly, the rollout of Elmer will greatly assist in information/intelligence interrogation and largely obviate the need for search requests.

46. **Automation**: Perhaps not surprisingly (though disappointing nonetheless), only four LEAs reported that any part of the information evaluation/intelligence development process is automated. Automation in this case refers to automated database checks (i.e. checking one or more names or addresses against multiple databases at once). While allowing for automation likely has significant up-front costs, it also likely has considerable savings through massive efficiency gains on the back-end. It seems legitimate that at least national database checks should be automated, such as PNC and HMCE's Cedric/Centaur (KPMG called for this in its 2003 report). Hits could be highlighted in Elmer when rolled out (though this would take some time, perhaps several years, to develop). This reinforces calls made in Bichard (2004) for national IT development along the lines of Scotland (with its Scottish Intelligence Database; the SDEA was one of the respondents noting automation in its SARs processes.

47. **Information Technology**: The IT approaches used by most LEAs to manage SARs are extremely limited. The majority of LEAs employ Microsoft Word and/or Microsoft Excel to track allocation of a received SAR to the responsible staff member (who will evaluate the information). A limited number of LEAs use true case management systems. Alternatively, a very small number of LEAs do little but print and file hardcopies. Elmer will not be of much use in terms of work-load/case management, as Elmer is not a case management system. There may be a need for a standard case management approach for SARs (and broader LEA work). LEAs were also asked if they could easily cross-reference a SAR against other SARs with their current systems/approaches. More than 80 percent responded in the affirmative. But it seems very unlikely that those LEAs using Word/Excel/hardcopies are maximising the investigative benefits of SARs, as it appears improbable that SARs can be efficiently interrogated/analysed in this fashion.

48. **Force intelligence**: The vast majority of LEAs indicated that SARs are entered on wider force intelligence systems (national systems for the national LEAs). Just under two-thirds of the 49 LEAs log only those SARs which undergo intelligence development (i.e. those clearing the information evaluation hurdle) on force intelligence systems. As noted, these will include SARs relating to known nominals, to ongoing investigations, or with other positive database hits. Nearly one-third of LEAs appear to log *all* SARs received. To protect the confidentiality of the information, most LEAs only place interest markers on force intelligence systems. These inform other LEA staff only that intelligence is held on the individual in question; interested parties must contact the FIU/FIDU for further information. While unconfirmed, there do seem to be a few examples of complete unsanitised SARs being placed on force intelligence systems. Once on FIB systems, these SARs may have been used without the knowledge (and associated feedback) of the initial SARs recipient. On the impact of the Elmer rollout: while having Elmer in FIBs will clearly increase SARs' contribution to force intelligence work, in the absence of truly interconnected IT systems, FIBs may still wish to somehow (e.g. subject names) load SARs onto FIB systems to allow for bulk searching and cross-checking.

49. **Guidance/training/advice**: LEAs receive only limited guidance from external sources on SARs processes and procedures. NCIS provides guidance on the confidentiality and sensitivity of SARs in both its training for the Elmer rollout and in work released through ACPO (this subject is of critical importance). ARA, which has the statutory responsibility under POCA for the training and accreditation of financial investigators, discusses SARs—though not in great detail—in its training courses for FIs (advanced courses, like the money laundering course, go into far greater depth). LEAs were asked about guidance; most reported that they received little or no guidance/training/advice. This seems to imply that existing NCIS/ACPO/ARA input is insufficient. A fair number of LEAs suggested that they would like more in-depth guidance on how to get the most out of SARs, including with turning confidential information into usable intelligence, data mining, best practice, and minimum work required. Several LEAs noted an obvious but oft-forgotten point that due to resource limitations, training must be very relevant to daily lives. Several LEAs expressed the desire for guidance to be handed down from ACPO and/or the Home Office on what *exactly* they should be doing with SARs and how SARs should be used. Additional comments received suggested that LEA staff were not sufficiently prepared for consent

and all that that civil decision implies (though they now appear to have things under control).

3. Uses of SARs (Outcomes)

50. Of the 249,244 SARs received in 2003 and 2004, 101,567 (40.8 percent) were disseminated to the 49 primary LEA users for action. These include LEA-bound consents and SARs which have been copied to (i.e. sent to) more than one LEA, perhaps because it was unclear if a SAR related to one location or another, or one type of criminality or another. These exclude, however, SARs related to terrorism and various other sensitive issues; SARs destined for overseas jurisdictions; SARs sent out in bulk backlog-clearing exercises (like the 2003 KPMG recommendation to clear the 2002/2003 backlog of SARs by sending them to LEAs on CD-ROMs); and SARs sent to NCIS units other than SFI.[44] Of the 101,567 SARs disseminated to the 49 primary users in 2003-2004, some 72,375 SARs were original disseminations (71.3 percent of the 101,567—which represents some 29 percent of the SARs received by NCIS in 2004-2004), while 29,192 SARs were copied-to disseminations (29.7 percent of the 101,567—which represents some 12 percent of the SARs received by NCIS in 2003-2004; see Table 3; see also Table 2, page 22, for information on allocations and disseminations of SARs by LEA). The majority of copied-to disseminations were sent to HMCE, MPS, and Inland Revenue (representing some 55.3, 14.3, and 11.4 percent of 2003-2004 copied-to disseminations, respectively).

51. So how were the SARs used in the fight against crime? Quantitative and qualitative data are used to triangulate findings. This section begins with a discussion of the availability of quantitative data (outcomes metadata), followed by presentations of quantitative and qualitative findings. The section closes with a discussion of the uses of SARs by NCIS.

[44] CD-ROMs were sent to LEAs in the KMPG backlog-clearing exercise. Further, after the June 2004 reduction of nonconsent disseminations, three LEAs—Cheshire Constabulary, Merseyside Police, and the MPS—took NCIS up on its offer to send semi-regular CDs containing those nonconsent SARs relevant to LEAs (curiously, other LEAs did not request this of NCIS). SARs sent out in this manner were not included in the statistics provided to the author by NCIS on SARs disseminations. Ignoring these particular SARs might render certain calculations inaccurate. But there are mitigating factors which suggest that this is less of a worry—at least with calculations. Not all LEAs even opened the KPMG CD. Some did not for resource reasons, or were simply uninterested (sadly); others could not, reporting that the CDs were provided in a computing format that was incompatible with their systems. And on the subject of the CDs sent to the three LEAs after June 2004, it appears that some of the information was sent to these LEAs not in calendar year 2004, but in 2005. Along these lines, the number of total SARs disseminated to the 49 LEAs in 2003 is probably more on the order of 80,000-100,000 (some of which will have been 2002 SARs), with 40,000-45,000 SARs disseminated in 2004. Because this could not be validated, calculations involving total disseminations will slightly over- or under-estimate the true situation (depending on the type of calculation). This is only an issue with tables/figures specifically drawing on NCIS-provided disseminations, not the information from LEAs.

Table 3. Annual Receipts and Disseminations of SARs by NCIS to LEAs, 2003-2004

Variable	*2003*	*2004*	*Total*
SARs received by NCIS	94,708	154,536	249,244
SARs allocated to the 49 primary users	97,677	133,133	230,810
Total SARs disseminated to the 49 primary users	66,098	35,469	101,567
Original disseminations	45,129	27,246	72,375
Copied-to disseminations	20,969	8,223	29,192

Source: NCIS. Disseminations exclude SARs related to terrorism and various other sensitive issues; SARs destined for overseas jurisdictions; SARs sent out in bulk backlog-clearing exercises (see footnote 44); and SARs sent to NCIS units other than SFI. The figure for 2003 allocations is slightly larger than the 2003 SARs received by NCIS; NCIS theorises that this is due to backlogged SARs being entered since the 2003 receipt figure was published. The figure for 2004 allocations slightly under-represents the number allocated to the 49 primary users, likely because while recorded as received, a backlog of SARs had not been entered into the system (and could not thus be automatically allocated to an LEA). SARs allocated to the 49 LEAs should not equal SARs received, though; some SARs will "belong" to LEAs other than these 49.

52. **Outcomes metadata**: LEA data on the uses of SARs are disappointingly limited. True, the LEA survey explored very precise concepts—including those aforementioned concepts called for by the FATF (through recommendation 32)—in order to understand both the information maintained and the broader information management practices of LEAs.[45] Even for those LEAs with strong record-keeping tendencies, it was expected that many concepts would be too specific. Further, responding to surveys is not the core responsibility of LEAs. As such, only information which was readily available was requested. A number of LEAs indicated that they could dig through their records by hand to provide some of the information (but didn't); this is discussed below. Table 4 sets forth the number of LEAs providing a numerical response—as opposed to saying *not readily available*—for each variable captured in the LEA survey on nonconsent and consent SARs (out of a total of 49 LEAs). All things considered, however, a considerable—and discouraging—number of data points for both nonconsent and consent outcomes were classified by LEAs as *not readily available*.[46] The most difficult variables to come by appear to be *number of nonconsents relating to an existing recorded crime* and *number of nonconsents resulting in a crime being recorded*. These questions relate specifically to Home Office crime recording rules, and were suggested by one of the LEAs piloting the survey. It may be the case that these concepts are far too specific, or perhaps too complicated, for most LEAs with their very limited record-keeping abilities.

[45] The outcome queries concentrated on those concepts commonly referred to by the FATF (Reuter and Truman's "intermediate measures"). Certain concepts were not included, though not for lack of interest; these included queries on the use of production orders, arrests, and the number of SARs received on the same subject. Fewer concepts were recorded with consents, as they are generally regarded as more quick-and-dirty than nonconsents and are often treated somewhat differently (several of the nonconsent concepts may have been applicable, however).

[46] In fact, 63.3 percent of the total number of nonconsent data points and 56.3 percent of the total number of consent data points in the survey were classified as not readily available by the 49 LEAs.

Table 4. Annual Nonconsent and Consent Outcomes Metadata, 2003-2004

	Number and percent of the 49 LEAs for which information was available			
Variable	*2003*		*2004*	
Nonconsent SARs				
Total number of nonconsent SARs **received**	31	63.3%	36	73.5%
Number of nonconsents undergoing **initial checks**	30	61.2%	32	65.3%
Number of nonconsents **investigated beyond initial checks**	17	34.7%	22	44.9%
Number of nonconsents **launching a proactive investigation**	16	32.7%	18	36.7%
Number of nonconsents **relating to an existing recorded crime**	10	20.4%	14	28.6%
Number of nonconsents **resulting in a crime being recorded**	10	20.4%	13	26.5%
Number of nonconsents contributing to a **prosecution**	13	26.5%	18	36.7%
Number of nonconsents contributing to a **conviction**	13	26.5%	15	30.6%
Number of nonconsents contributing to a **cash seizure**	18	36.7%	21	42.9%
Number of nonconsents contributing to a **cash forfeiture**	17	34.7%	19	38.8%
Number of nonconsents contributing to a **restraint**	15	30.6%	19	38.8%
Number of nonconsents contributing to a **confiscation**	13	26.5%	15	30.6%
Amount of cash **seized** through nonconsents (GBP)	18	36.7%	19	38.8%
Amount of cash **forfeited** through nonconsents (GBP)	17	34.7%	18	36.7%
Amounts **restrained** through nonconsents (GBP)	14	28.6%	16	32.7%
Amounts **confiscated** through nonconsents (GBP)	13	26.5%	14	28.6%
Consents SARs				
Total number of consent SARs **received**	24	49.0%	33	67.3%
Number of consents **granted**	21	42.9%	29	59.2%
Number of consents **refused**	23	46.9%	32	65.3%
Number of consents contributing to a **prosecution**	18	36.7%	26	53.1%
Number of consents contributing to a **conviction**	16	32.7%	24	49.0%
Number of consents contributing to a **cash seizure**	16	32.7%	26	53.1%
Number of consents contributing to a **cash forfeiture**	16	32.7%	23	46.9%
Number of consents contributing to a **restraint**	16	32.7%	23	46.9%
Number of consents contributing to a **confiscation**	16	32.7%	20	40.8%
Amount of cash **seized** through consents (GBP)	18	36.7%	24	49.0%
Amount of cash **forfeited** through consents (GBP)	16	32.7%	19	38.8%
Amounts **restrained** through consents (GBP)	18	36.7%	22	44.9%
Amounts **confiscated** through consents (GBP)	16	32.7%	22	44.9%

Source: Survey of LEAs. N=49 LEAs overall. Not all data points come from the same LEAs. For example, an LEA may have stated that the number of nonconsent SARs received *was not readily available, but may then have provided figures for the* number of nonconsents launching a proactive investigation *(perhaps because this was zero, and was thus easily knowable). Fewer concepts were recorded with consents, as they are generally regarded as more quick-and-dirty than nonconsents and are often treated somewhat differently. Lastly, the Inland Revenue has powers others do not, including Hansard valuations and Avoidance (fraud work opened under IR code of Practice 8); these are not captured above, though SARs contribute to such work.*

53. Of those LEAs providing limited or no information, the vast majority cited limited IT capacity, followed by lack of resources (particularly clerical support). Most LEAs use Word or spreadsheet applications to manage the SARs process in terms of tracking officers' workloads (and sometimes the status of initial checks), but no information is captured on outcomes (see page 28 for more on LEA IT solutions). A small number of LEAs could not separate nonconsent and consent figures, as they used common IT approaches with no consent identifier. On a positive note, several LEAs had begun new record-keeping procedures (with new IT) in the last year; they could not provide statistics on outcomes yet, but hope to do so in the future. There already does seem to be an improvement in the 2004 data. This may be due to more managerial interest in financial investigation.

54. It's not that the outcomes data were impossible to assemble: for the LEAs with limited or no information on outcomes, most stated that the information was indeed available, just not in an easily obtainable format (though eight of the 49 LEAs indicated that the specific missing variables were really not known at all). Difficulty with outcomes information appears to have been expressed by the units whose remit is limited to intelligence development: as all packages are sent elsewhere in the organisation for action, these units are dependent on others (perhaps nationwide) for feedback. Six LEAs claimed that statistics were not readily available for *any* of the variables, including the number of SARs received from NCIS for each year.

55. LEAs were asked in the survey whether they could easily track the progress of a SAR from the date of receipt to eventual outcome, such as prosecutions/convictions. Forty of the 49 LEAs noted that they could easily track the progress of SARs to outcomes, yet this does not appear to be the case (somewhat surprisingly, the ability to easily track outcomes appears uncorrelated with the actual provision of outcomes statistics, above). It is difficult to imagine that there are LEAs which keep *no* management information whatsoever, not even the number of SARs received from NCIS. This may all be suggestive of a disdain for record-keeping—a short-sighted position, given that it's very difficult to argue for more resources (or to criticise facets of the regime) without proof of the problem. This may also be suggestive of a lack of clerical resources and/or limited IT fluency (most LEAs who indicated they could track SARs from cradle to grave described some sort of IT solution; can these IT platforms really not provide aggregate statistics at all?).

56. LEAs were also asked what could be done to allow for the provision of outcomes data. Most suggested the modification of existing IT systems; many went so far as to suggest the introduction of a uniform, purpose-built IT solution (like a case management system for use nationwide), and greater resources to cope. A number of LEAs sensibly noted that while they needed to adapt their IT systems and procedures, they were awaiting the nationwide rollout of Elmer to see how things would play out. And a not-uncommon complaint was that LEAs had never been told exactly what data to keep (and that they had not been asked for such information before). In fact, several LEAs noted that they simply wanted to be told *exactly* what was expected, and they'd change their systems accordingly.

57. These last comments seem a bit disingenuous; further, they flag up a disconnect in the regime between policy-makers and LEAs. It is not entirely the case that information on outcomes has never before been requested. KPMG (2003) and Gold and Levi (1994) both searched for outcomes information (and KPMG included some outcomes questions similar to those used here in its survey of LEAs). KPMG (2003) in particular represents a publication which virtually all SARs-related LEA staff should be familiar with. Moreover, the FATF and others, including the IMF and World Bank (who now draw on the FATF's assessment methodology in their work on member countries' AML regimes), clearly refer to the need for outcomes statistics in various publications. And it seems eminently reasonable for industry and government to want to know what the AML regime is delivering, even if the indicators of performance are imperfect and in no way capture perhaps the regime's most powerful component, deterrence. LEAs may (and do, at least anecdotally) feel that feedback on outcomes is the role of NCIS—but this still requires near universal uptake of the feedback process by LEAs. And perhaps it is unrealistic to expect law enforcement officers to appreciate international standards and guidelines, along with all of the other, perhaps more relevant knowledge which affects daily responsibilities (e.g. knowledge of the Regulation of Investigatory Powers Act 2000, POCA). But the UK is active in the work of the FATF, IMF, and World Bank, so at least some policy-makers in the Home Office and HMT should be fully aware of the need for outcome statistics—and the dearth thereof. This awareness has not translated into action in LEAs, ACPO, and NCIS—or for an appreciation of the need for information on outcomes. This may result from the lack of a clear owner of the UK's AML regime, particularly with regard to all things SARs.

58. **Outcomes—Quantitative data**: Some LEAs did, of course, provide outcomes data (presented in Table 5, below); quantitative and qualitative data are used to triangulate findings. So how were the disseminated SARs used by the LEAs? Several important caveats must be considered when interpreting these data. First of all, many LEAs provided little or no data, so the results do not represent the situation in its entirety; these figures clearly underestimate the true SARs-related outcomes. Critically, a number of LEAs providing no data on certain variables discussed examples of SARs-related successes of often considerable magnitude. A number of LEAs *do* appear to be doing good and often excellent work with SARs, at least according to one-off examples given to the author or anecdotal information and the perceptions of various respected people within the regime. Some examples are contained in Appendix 1; others are of interest but remain *sub judicae* (and out of the public domain); and still others are of interest but relate to cases in which the use of one or more SARs has not been made public. Regardless, not all data points here come from the same LEAs. For example, an LEA may have stated that the *number of nonconsent SARs received* was not readily available, but may then have provided figures for the *number of nonconsents launching a proactive investigation* (perhaps because this was zero, and was thus easily knowable). Many LEAs provided information on seizures, but could not provide information on forfeitures (the same goes for prosecutions/convictions and for restraints/confiscations—though funds need not be restrained prior to confiscation). Internal consistency is sometimes lacking: for example, for several LEAs, the number of consents granted plus consents refused does not add up to the number of consents received. On external consistency, some LEAs reported receiving more SARs than NCIS reported disseminating to them, though this is very likely explained by search requests and bulk disseminations. Data were not validated. **In any case, figures received may not be representative of the broader population of all 49 LEAs**.

59. Furthermore, as noted in Chapter III, there are no perfect measures of outcomes (see pages 18-19). To reiterate, when interpreting the outcomes figures it is important to consider the following: uses of SARs are not mutually exclusive; many SARs together will be used to illustrate the pattern of offending of a lone individual; many SARs will be received relating to people already under investigation; and outcomes measures cannot illustrate the extent of the deterrent effect of the regime. No allowances have been made here for time: SARs disseminated in one period may be put to use several months or even years later. Because there is only limited understanding of the extent to which this occurs, it seems prudent to simply present/compare 2003 outcomes with 2003 disseminations and 2004 outcomes with 2004 disseminations.

60. What do these data imply **when viewed in their totality**, as in Table 5? The problem is that **they may not imply much in this aggregate format—at least not in illustrating the attrition of SARs from receipt to outcomes—because so many different concepts contain data provided by different LEAs**. Comparisons drawn here are suggestive of comparisons between apples and oranges (i.e. they're meaningless). The safest points to discuss may concern the amounts recovered through nonconsents and consents. There are still more responding LEAs on certain variables than others, but these data do seem to suggest that perhaps consent SARs are more efficient than nonconsents in terms of asset recovery. A number of LEAs currently hold a very favourable view of consents, and see them having the greatest impact. This should come as no surprise: consents represent current information on pending money movements. These LEAs discussed some high-profile uses of consents, some of which are not captured in the data. Of course, as with everything here, one or two spectacular cash seizures or confiscations can skew the results dramatically.

Table 5. Annual Nonconsent and Consent Outcomes, 2003-2004

	2003			*2004*		
Variable	***N***	***Sum***	***Mean***	***N***	***Sum***	***Mean***
Nonconsent SARs						
Number of nonconsent SARs **received**	31	36,372	1,173.3	36	32,567	904.6
Number of nonconsents undergoing **initial checks**	30	19,414	647.1	32	20,155	629.8
No. of nonconsents **investigated beyond initial checks**	17	7,951	467.7	22	8,855	402.5
No. of nonconsents **launching a proactive investigation**	16	297	18.6	18	774	43.0
No. of noncnsnts **relating to an existing recorded crime**	10	29	2.9	14	402	28.7
No. of nonconsents **resulting in a crime being recorded**	10	26	2.6	13	31	2.4
Number of nonconsents contributing to a **prosecution**	13	57	4.4	18	229	12.7
Number of nonconsents contributing to a **conviction**	13	26	2.0	15	28	1.9
Number of nonconsents contributing to a **cash seizure**	18	33	1.8	21	32	1.5
Number of nonconsents contributing to a **cash forfeiture**	17	30	1.8	19	26	1.4
Number of nonconsents contributing to a **restraint**	15	29	1.9	19	31	1.6
Number of nonconsents contributing to a **confiscation**	13	28	2.2	15	30	2.0
Amount of cash **seized** through nonconsents (GBP)	18	£435,445	£24,191	19	£106,145	£5,587
Amount of cash **forfeited** through nonconsents (GBP)	17	£215,145	£12,656	18	£28,145	£1,564
Amounts **restrained** through nonconsents (GBP)	14	£4,760,000	£340,000	16	£4,561,000	£285,063
Amounts **confiscated** through nonconsents (GBP)	13	£182,000	£14,000	14	£-	£-
Consents SARs						
Number of consent SARs **received**	24	3,457	144.0	33	4,854	147.1
Number of consents **granted**	21	2,162	103.0	29	3,467	119.6
Number of consents **refused**	23	84	3.7	32	416	13.0
Number of consents contributing to a **prosecution**	18	1	0.1	26	16	0.6
Number of consents contributing to a **conviction**	16	-	-	24	8	0.3
Number of consents contributing to a **cash seizure**	16	3	0.2	26	17	0.7
Number of consents contributing to a **cash forfeiture**	16	3	0.2	23	2	0.1
Number of consents contributing to a **restraint**	16	4	0.3	23	26	1.1
Number of consents contributing to a **confiscation**	16	1	0.1	20	6	0.3
Amount of cash **seized** through consents (GBP)	18	£5,931,247	£329,514	24	£1,734,586	£72,274
Amount of cash **forfeited** through consents (GBP)	16	£20,000	£1,250	19	£30,000	£1,579
Amounts **restrained** through consents (GBP)	18	£4,690,000	£260,556	22	£15,575,900	£707,995
Amounts **confiscated** through consents (GBP)	16	£35,000	£2,188	22	£4,808,801	£218,582

Source: Survey of LEAs. The N columns provide variable-specific numbers of respondents (out of 49 total respondents). ***Figures should be interpreted with great care: not all LEAs provided quantitative data, and not all data points come from the same LEAs****. For example, an LEA may have stated that the* number of nonconsent SARs received *was not readily available, but may then have provided figures for the* number of nonconsents launching a proactive investigation *(perhaps because this was zero, and was thus easily knowable). Moreover, many LEAs provided information on seizures, but could not provide information on forfeitures (the same goes for prosecutions/convictions and for restraints/confiscations—though funds need not be restrained prior to confiscation). Fewer concepts were recorded with consents, as they are generally regarded as more quick-and-dirty than nonconsents and are often treated somewhat differently. Lastly, the Inland Revenue has powers others do not, including Hansard valuations and Avoidance (fraud work opened under IR code of Practice 8); these are not captured above, though SARs contribute to such work. Data were not validated.*

61. **Things become somewhat clearer and less tentative, however, when looking *only* at those LEAs who provided data for *all* of the major concepts** (allowing like-with-like comparisons, notably those relating to receipts and outcomes). **These findings may certainly *not* be representative of the broader population of 49 LEAs, but at least the contribution of SARs to various outcomes can more or less be followed**. Unfortunately, only seven LEAs—all smaller territorial police forces from England & Wales—provided data on *all* of the outcomes concepts captured in the survey. Further, there is some evidence of double counting within recovery figures, which could not be confirmed. Total values for concepts like number of SARs relating to a prosecution and/or cash seizure and/or restraint (for nonconsents + consents) are very low (at six, zero, and two, respectively, all from 845 SARs received; not shown).

62. Along these analytical lines, Table 6 presents information on nonconsent investigative processes for the 14 LEAs (comprising territorial police and two national LEAs) who provide figures for all of the relevant variables (though this is not to suggest that a one-by-one approach to SARs development is the best use of resources; there is indeed a place for deeper information interrogation). While likely not necessarily representative of the larger population of the 49 LEAs, it is interesting to follow the attrition of SARs through the process. The vast majority of SARs appear to undergo initial checks (i.e. information evaluation). A smaller percentage of the SARs received is investigated beyond initial checks (i.e. intelligence development). And a considerably smaller percentage of SARs received launch a proactive investigation (though this has nothing to do with those SARs relating to ongoing investigations). These percentages are captured in two different ways: in aggregate percentages (such that nonconsent SARs undergoing initial checks as a percentage of SARs received in the *overall* column equals 10,794/12,016; and in the *LEA mean* column, the percentage is first calculated by LEA, and then the mean percentage is taken). Either way, and bearing in mind all of the caveats on information interpretation, nonconsent SARs launching a proactive investigation as a percentage of nonconsents received seems fairly low. This should come as no surprise: many LEAs appear to only work-up SARs relating to ongoing investigations, so few resources seem to be used in developing proactive cases.

Table 6. Annual Nonconsent Investigative Processes for 14 LEAs, 2004

Variable	*Number of SARs (Total for the 14 LEAs)*	*As a percentage of SARs received (overall)*	*As a percentage of SARs received (LEA mean)*
Nonconsent SARs allocated	27,185		
Nonconsent SARs disseminated	12,788		
Nonconsent SARs received	12,016	100.0%	100.0%
Nonconsent SARs undergoing initial checks	10,794	89.8%	92.0%
Nonconsents investigated beyond initial checks	8,030	66.8%	25.7%
Nonconsents launching a proactive investigation	763	6.3%	6.7%

Sources: NCIS (for allocations and disseminations); and survey of LEAs. N=14 LEAs (who provide figures for all of the data points). The 14 LEAs include territorial police and two national LEAs. Nonconsent SARs undergoing initial checks as a percentage of SARs received in the overall *column is computed as 10,794/12,016; and in the* LEA mean *column, the percentage is first calculated by LEA, and then the mean percentage is taken.*

63. A separate analysis was undertaken to explore the percentage of overall 2004 cash seizures and confiscations which relate to SARs, as reported by 12 and 11 LEAs (all territorial police forces) responding to cash seizure and confiscation queries, respectively (see Table 7). Again, these findings may in no way be generalisable to the broader population of 49 LEAs. On average, 1.6 percent of cash seizures and 3.5 percent of confiscations appear to be SARs-related, at least for these 12 and 11 LEAs. The maximum percentages are 11.5 percent and 38.6 percent for SARs-related cash seizures and confiscations, respectively. Perhaps these are more indicative of the levels that could be expected with more zealous use of SARs. Two data points were excluded from the cash seizure and confiscation comparisons (one from each), as they related to SARs-related activity of greater than 100 percent—an impossibility. Note that 2004 confiscation data are for the 2004/05 fiscal year; these data are used as proxies for the calendar year data. Further, only 10 months of data have been used (April 2004-January 2005). The point is not to establish exactly the percentage of each relating to SARs, but rather just to get an indication of the scale.

Table 7. Annual SARs-Related Cash Seizures and Confiscations as a Percentage of Cash Seizures and Confiscations, 2004

Variable	*N (LEAs)*	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
SARs-related cash seizures as a percentage of cash seizures by LEA	12	0.0%	11.5%	1.63%	3.5048
SARs-related confiscations as a percentage of confiscations by LEA	11	0.0%	38.6%	3.51%	11.6529

Sources: Survey of LEAs; and JARD (provided by the Home Office). Overall cash seizure data relate only to LEAs in England & Wales. Overall confiscation data relate to LEAs in England & Wales and PSNI. Confiscation data are for the 2004/05 fiscal year, and include only April 2004-January 2005); they are used as a proxy for the 2004 calendar year data. The LEAs include territorial police.

64. That so few LEAs provided data on certain specific concepts certainly implies that more than half of the LEAs are not represented in much of the debate. It is very possible that these LEAs would change the thrust of the story—and some LEAs appear to be doing good work with SARs. But bearing in mind the limitations on data interpretation, some tentative conclusions may be drawn. **The over-arching and unsurprising conclusion is that <u>for those few LEAs providing data</u>, SARs appear to be considerably under-utilised**. SARs deter some money laundering—but it is *not* the case that *all* offenders engaging in money laundering activity are or will ever be completely deterred by the SARs regime. As such, SARs should indeed lead to criminal justice outcomes. It is likely difficult to know good performance when one sees it: there is a theoretical maximum on the number/percentage of SARs contributing to X or Y criminal justice outcome, of course, because many SARs will relate to innocent people, many to people not worth pursuing, and many to the same individuals (who may fall in the innocent/not worth it categories). So it may be the case that excellent performance on, say, SARs launching proactive investigations as a percentage of SARs received is 40 or 50 percent or even (far) less. But that doesn't imply that it should be too difficult to know *weak* performance when one sees it. And look: for the 14 LEAs providing data (from Table 6), nonconsent SARs launching a proactive investigation represent only some six or seven percent of nonconsents received? For the 11 LEAs providing data (from Table 7), the mean

percentage of SARs-related confiscations as a percentage of confiscations by LEAs is 3.5 percent? For the 26 LEAs providing 2004 data (from Table 5), only 17 consent SARs contributed to a cash seizure? For the 15 LEAs providing 2004 data (again from Table 5), only 30 nonconsent SARs contributed to a confiscation? Even bearing in mind all of the relevant caveats, these figures seem suboptimal.

65. Of course, it could be the case that the SARs examined by the handful of LEAs providing data (and specifically for those providing data for Tables 6 and 7) showed little promise. That is, perhaps it's not that SARs were under-utilised, but rather that the SARs were largely unrelated to crime. So is there any external source that might confirm under-utilisation?[47] Specifically, what percentage of SARs appear innocent, and what percentage crime-related? In the event, the London RART evaluated a sample of SARs to determine the extent to which SARs corresponded to known/suspected individuals (this research was carried out in part to assist the present research). The sample contained 200 nonconsent SARs selected in November 2004 solely on the basis of postcode (for one London borough). The SARs themselves date from 2004. The sample was searched against three external databases to check for hits against existing sources of information. These databases included the MPS Crime Reporting Information System (CRIS), PNC, and the MPS Criminal Intelligence system (CRIMINT) Level 1 and Level 2. The results are presented in Table 8, below.[48]

66. This London RART sample is likely not overly generalisable, as the SARs all concern a fairly crime-ridden area. And an unspecified but small number of SARs were thought to relate to the same subject, so there will be some minor double-counting. Some 46.5 percent of the sample had hits on CRIMINT Level 1; 29.5 percent had hits on CRIMINT Level 2; 20.5 percent had hits on PNC; and 8.5 percent had its on CRIS. While many of these hits will be for relatively minor things, the analysis illustrates that these SARs are indeed suggestive of at least some criminality. This criminality did not appear to already be under investigation. It seems more than feasible that a number of proactive investigations could potentially be launched on the back of this initial work (perhaps more after more in-depth analysis).

[47] The NCIS regional office in Wales (in conjunction with the NCIS officer in the Wales RART) is conducting an ambitious (and exciting, as far as the present research is concerned) assessment of the impact of SARs on the ACPO Wales Region. According to the project terms, "the assessment will analyse how the dissemination of SARs to Welsh law enforcement agencies has benefited financial investigations, assisted in identifying and recovering the proceeds of crime and affected the capability of criminals and the viability of criminal business. The assessment will cover the period from the inception of POCA in February 2003 to February 2005." It was hoped that assessment findings would be available for discussion in the present report, not least because findings would provide extremely useful supplemental information on the uses to which SARs are put. Unfortunately, the assessment has been put on hold for several months.

[48] It was expected that other LEAs might be in a position to provide similar data. An informal poll of LEAs attending the FIWG meeting in Guernsey was carried out; only one LEA replied in the affirmative, but then realised that data were unlikely to be of use for various reasons.

Table 8. Database Hits on a Sample of SARs from a London Borough

System	*Hits*	*Percentage of sample with hits*	*Notes*
CRIS	17	8.5%	No fuzzy searching capability and only exact matches against names were counted. A hit implies that the subject is suspected of at least one specific reported crime. Also, 22 percent of the sample were known to CRIS as victims, witnesses, etc.
PNC	41	20.5%	Only exact matches on names were counted.
CRIMINT Level 1	93	46.5%	Matches to exact names or addresses were counted, as either could prove to be useful.
CRIMINT Level 2	59	29.5%	Same as with CRIMINT Level 1. Level 2 covers people and places of interest to pan-London policing units and reflects a higher level of possible criminality.

Source: London RART. N=200 SARs. An unspecified small number of SARs were thought to relate to the same subject, so there will be minor double-counting.

67. Along similar lines, the MPS FIDU evaluated each nonconsent SAR received by the MPS in a one-week period also, coincidentally, in November 2004 (see Table 9). These SARs were not filtered by NCIS in any way; but rather were received in bulk on a CD-ROM. All SARs in the sample of 551 were examined (implying a close reading of the reason for suspicion and other details). Some 134 SARs (24.3 percent) were dropped from the sample as they were misallocated to the MPS. The remaining 417 SARs underwent both a close reading and a PNC search. Of these, 97 (23.3 percent of the 417) were SARs which related to previous SARs in that they represented information on the same individual. This is particularly useful information; this appears to be the only figure on the percentage of SARs which relate to previously disclosed-upon individuals. The 97 SARs relating to previous SARs had 11 hits on PNC (11.3 percent). The remaining 320 SARs had no connection to previous SARs. Fifty-eight of these 320 had hits on PNC (18.1 percent). Of the 417 correctly allocated SARs, 69 (16.5 percent) had positive PNC hits. These findings are not as powerful as those of the London RART. But this effort represents nothing more than PNC checks. If the London RART example is any guide, local force intelligence databases would likely yield higher levels of hits—not to mention the reason for suspicion—and thus would yield at least *some* potential proactive investigations.

Table 9. PNC Hits on a Sample of SARs from the MPS FIDU

Variable	*SARs*	*Percentage of total SARs*	*PNC hits*	*Percentage with PNC hits*
Total SARs correctly allocated	417	100.0%	69	16.5%
SARs on previously-disclosed upon individuals	97	23.3%	11	11.3%
New SARs	320	76.7%	58	18.1%

Source: MPS FIDU. N=417 SARs. Note that 551 SARs were received overall, of which 134 (24.3 percent) were misallocated.

68. **Outcomes—Qualitative data**: The outcomes data provided to varying degrees by the 49 LEAs are incomplete, of course, so on this basis alone it isn't appropriate to claim that SARs are broadly under-utilised by LEAs nationwide. But the LEAs themselves concur: **by their own admission, 38 of the 49 LEAs—more than 77 percent—stated that SARs were under-utilised in their unit**. Of those stating that the utilisation of SARs in their unit was just right, several suggested that this was because any increase in SARs-related work would strain resources too tightly (and that resources were already under pressure). The fact that SARs are under-utilised was further confirmed by conversations with knowledgeable members of the law enforcement community and in site visits (not to imply that all site visit participants are under-performing).

69. The question then becomes why: why are SARs under-utilised by LEAs? LEAs were asked if the uses to which SARs were put—and thus outcomes—were limited in their units by various factors. Only two LEAs suggested here that the uses to which SARs were put were not limited at all (in contrast to the twenty-something percent of LEAs saying that SARs use was just right in the preceding question). Of the remaining 47 units, nearly 90 percent reported that the uses to which SARs were put were constrained by resource limitations in their unit. Rarely will organisations forego the opportunity to ask for more resources when given it. In this case such claims appear appropriate. A large number of comments received suggested that limitations on SARs-development resources prevented LEAs from working up targets unless they were known nominals. Several LEAs reported that all they could do was search for SARs relating to existing investigations—and that SARs just weren't getting the attention they deserved. Some LEAs rationally noted that they found it difficult to justify allocating scarce resources on the back of only one piece of information. This is not to argue for a *massive* increase in SARs-related resources for each LEA. One of the responding LEAs probably gets it right with the following statement:

> It's all a matter of degree. Unlimited additional resources would maximise their potential but we need to concentrate on improving things first. How about better systems and a moderate increase in resources, matched by a realisation that judicious selection of a significant SAR, followed by adequate attention to and interest in it might actually create a worthwhile result.

70. LEAs went on to cite further reasons why the uses to which SARs were put were limited. These included: difficulties in selling SARs-based jobs to operational teams (32 percent); no clear suspicion contained in SARs (32 percent); IT systems in their units (19 percent); the fact that LEAs were getting fewer nonconsent SARs from NCIS since June 2004 (15 percent); and the fact that SARs upon receipt were several months old (9 percent). These were not mutually exclusive, such that LEAs could select any of the reasons that applied to them (the latter two were identified by the LEAs in open-text fields).

71. It's no secret that LEAs seem to work on things that are measured, and ignore things that are not. No performance indicators of any value on SARs were identified anywhere. Some LEAs noted that they monitor SARs received from NCIS, though it is hard to imagine that this is useful for anything other than a work-load barometer (as opposed to a true performance monitor). Uses might be increased with appropriate performance indicators.

72. Finally, LEAs were asked for recommendations on improving the use and management of SARs. Their comments all reinforced thoughts set out above and discussed over the many preceding pages. LEAs suggested that sufficient resources be devoted to SARs; better IT solutions for case management and SARs analysis (including data mining tools and perhaps national IT solutions for the handling of intelligence); and full access to timely SARs from NCIS. LEAs also noted the need for LEA managers to continue to work toward the mainstreaming of POCA and financial investigation. And lastly, LEAs called for more education/training of the regulated sector, to ensure that little noise accompanied the SARs signal (i.e. to ensure that only SARs based on true suspicion were filed, not defensive or misguided reports).

73. **NCIS uses of SARs**: After years spent primarily inputting, processing/analysing, and disseminating SARs, NCIS SFI has entered the intelligence-development arena. SARs are used to generate or contribute to various tactical and strategic intelligence products within SFI.[49] While some are self-tasked, most SFI products are driven by national strategies—as set forth in the NCIS Service Plan—established by the Concerted Inter-Agency Criminal Finances Action Group (CICFA), the Concerted Inter-Agency Drugs Action Group (CIDA), the REFLEX Group (on illegal immigration and human trafficking), and the national firearms strategy. Current SFI work products range from problem profiles to current intelligence assessments (CIAs) to baseline assessments to target/nominal profiles, all of which contribute to the store of knowledge on money laundering.[50] While sensitive (products cannot be discussed in detail here), such products may examine how particular sectors are used to launder criminal proceeds, may identify emerging trends, and may suggest targets for tactical activity. Products are generally sent to FIBs and FIUs, though distribution lists are not fixed. Many of these products are sanitised and forwarded to industry. SFI also uses SARs to support Operation Payback initiatives in various regions, primarily with quick-and-dirty (yet useful) target lists and subject-of-interest lists. SARs are used in strategic research on various aspects of the regime (one such project focuses on consent SARS and their efficacy). Along these lines, the NCIS regional office in Wales is carrying out a broad analysis of the use and impact of SARs in Welsh LEAs (see footnote 47). Perhaps most interesting of all is some tactical work SFI is running on some significant targets. This type of work often involves 20-40 suspects in criminal networks, with sometimes hundreds or even thousands of SARs (informed by other sources of intelligence, of course).[51] Lastly, SFI plays a significant

[49] SARs are disseminated to NCIS units outside SFI; according to SFI, more than 34,000 SARs were disseminated to non-SFI units in 2003-2004 (of which some 800+ represent original disseminations, with the rest as copied-to disseminations). This research did not contact non-SFI units to explore how these SARs were used.

[50] *Problem profiles* identify specific areas or issues requiring operational attention or policy development; *current intelligence assessments* describe newly identified traits in criminal activity or assessments of current impacts against previously identified areas; *target profiles* identify specific individuals or entities for law enforcement attention; and *baseline assessments* capture baseline information on identified issues (NCIS, no date).

[51] The number of SARs used in intelligence products represents an interesting piece of management information which begins to shed some light on the use made of SARs. Unfortunately, NCIS keeps no record of the number of SARs used in the drafting of its products. Excluding the tactical work based on the many hundreds of SARs, most products appear to be based on limited numbers of SARs. Intelligence products do, of course, also draw from other NCIS databases/products and open-source information.

role in international work, through foreign financial intelligence unit requests for information, with the FATF, and in representing the UK in the Egmont Group. SARs may contribute to these international responsibilities.

74. A relevant question is this: are LEAs using the tactical and strategic products drafted by NCIS? LEAs were asked if they received such products and if they prioritised them. Most LEAs reported that they had received few if any SARs-based products from NCIS (the LEAs who did receive such products suggested that these were indeed prioritised in some way). To some extent this is a distribution issue: many such intelligence products will be released on a need-to-know basis. The majority of the products relate to national serious organised crime priorities, which will have little to do with most territorial LEAs. That said, those certain products intended for wider distribution to improve LEAs' AML capabilities do not appear to be getting to the troops in the trenches. Some LEAs felt this might be due to their own managers who received the products but did little with them. A general vibe was put out by many of the LEAs, though one perhaps biased by pre-existing enmity towards NCIS, that NCIS was/is answering questions nobody asked with its intelligence products (though the majority of these do seem to have been tasked by CICFA). If nothing else, this does all seem to be suggestive of the need for better communication between NCIS and LEAs.

4. Feedback from LEAs to NCIS/Industry

75. **Feedback from LEAs to NCIS**: NCIS maintains systems and protocols for receiving SARs-specific feedback from LEAs. Disseminated SARs are each accompanied by a feedback form through which LEAs can provide information on the usefulness of the SAR and the purpose, if any, to which it was put. The form also provides the opportunity to supply details of any outcomes and to pass on anything learned from the use of the SAR (e.g. modus operandi of the offender) for potential use in typologies. Information captured in the SAR feedback form is described in Table 10. Notable in the design of this form is that despite its depth (and perhaps over-zealous length), several important concepts are lacking, and there is an incomplete overlap with those concepts called for by the FATF (e.g. there is no mention of restraint/confiscation). Also, there is no easy way to capture the fact that the SAR in question links to previous SARs in some manner (NCIS will no longer capture links to previous SARs with the Elmer rollout, as LEAs will be able to conduct searches yielding this information). LEAs are encouraged to send feedback forms back to NCIS electronically (via the *money.web* extranet or secure email), though hardcopy feedback is accepted. Additional short forms are used for consent SARs: Document A records the consent decision (along with the reasoning behind the approval or denial of consent); Document B is completed by LEAs only in the case that consent is denied, and after 31 days have passed, describing the details of the investigation and any subsequent court orders applied for.

Table 10. SAR Feedback Form

Section/question	***Answer choices***
1. Initial assessment. Please select one of the following	Suitable (go to section 2) After evaluation deemed unsuitable (go to section 8) Insufficient data supplied (go to section 8) Requires allocation to another force area (go to section 8)
2. Source contacted. Disclosing institution has been contacted	[Check box]
3. Current status. Please select one of the following	Awaiting evaluation (no action initiated) Under active investigation or evaluation Complete (enter results in part 4)
4. Result/current progress. Please select at least one of the following	Disclosed transactions identified as proceeds of crime Other proceeds of crime identified as a result of investigation or evaluation Direct arrest (please give details in section 8) Assist arrest—other persons arrested (please give details in section 8) Realisable assets identified and value of assets No connection to crime at this time but still suspicious Funds not linked to criminality (please give details in sect. 8) Cannot progress because confidentiality will be broken Linked to an ongoing enquiry
5. Final assessment. Please select one of the following	Existing intelligence enhanced (info on local database supplemented) New intelligence (new record created on local database—no existing current record) After evaluation suggested reallocation to another government department (please specify a more appropriate investigator in sect. 8) Charged/summoned Convicted
6. Modus operandi	[Open-ended answer field]
7. Relevant investigation material. New nominals, companies, transactions, addresses or information records added by search request	[Check box]
8. Comments. Please include intelligence evaluation where appropriate	[Open-ended answer field]

Source: NCIS. This form is to be completed for all SARs; two additional short forms should be filled out for consent SARs.

76. Neither incentives nor sanctions are used to persuade LEAs to send feedback. NCIS staff suggested that there were no specific guidelines for LEAs regarding feedback provision, at least that they were aware of. LEAs are strongly encouraged to provide feedback to NCIS and reminders are given in various fora, such as the quarterly meeting of the national FIWG or through occasional visits by the SFI Collections team. The system was historically set up to chase feedback from LEAs at various intervals (via periodic emails); this facility has not been used for several years, as LEAs found it to be a cause of consternation as opposed to a useful reminder.

77. NCIS received 29,135 feedback forms from the 49 primary LEAs in 2003-2004, representing some 28.7 percent of the 101,567 SARs disseminated to these LEAs in the same period.[52] This is 40.3 percent of the 72,375 original disseminations (it is unclear whether the query providing feedback information captured feedback on the same SAR (perhaps filed by two organisations looking at the original and copied-to SARs). Also, it may be most appropriate to view feedback forms with a lag (viewing April forms received as a percentage of January SARs, for example), though this makes little difference to the 2003-2004 aggregate percentage (April 2003-December 2004). Moreover, the pattern of feedback received seems to track disseminations in the same month (suggesting to some extent that substance of the feedback will likely contain little on outcomes). Interestingly, despite suggestions to the contrary, a good number of LEAs provide feedback on a regular basis; 14 of the 49 LEAs provided feedback on more than 50 percent of the SARs disseminated to them in 2004. LEAs also almost universally supplied Document A recording the consent decision of all consents disseminated; 49 Document B forms were received between January and December 2004 (NCIS did not maintain this information prior to January 2004). Bearing in mind that Document B forms are only supplied to NCIS when consent is denied, a small number of Document B receipts was to be expected (though this figure of 49 forms does appear suboptimal). Feedback figures are presented in Table 11.

Table 11. Annual Feedback Sent from LEAs to NCIS, 2003-2004

Variable	***2003***	***2004***	***Total***
Feedback forms received by NCIS	18,849	10,286	29,135
Total SARs disseminated to the 49 primary users	66,098	35,469	101,567
Feedback as a percentage of these total disseminations	28.5%	29.0%	28.7%
Original SARs disseminated to the 49 primary users	45,129	27,246	72,375
Feedback as a percentage of these original disseminations	41.8%	37.8%	40.3%

Source: NCIS. Disseminated SARs exclude SARs related to terrorism and various other sensitive issues; SARs destined for overseas jurisdictions; SARs sent out in bulk backlog-clearing exercises (see footnote 44); and SARs sent to NCIS units other than SFI. Total SARs includes original disseminations plus copied-to disseminations.

[52] The SARs disseminated to the 49 LEAs is likely an underestimate because it doesn't include bulk disseminations. See footnote 44 for more information.

78. Disappointingly, NCIS seems to have done little with LEA feedback since end-2002/early-2003. NCIS states that feedback received may be used in the drafting of intelligence products/typologies which are disseminated to LEAs and occasionally to industry (often via *money.web*). But the use of feedback for intelligence products is an ad hoc use, and comments received indicate that feedback may play only a limited role in this regard. No systematic analyses based solely on feedback appear to have been carried out to understand the larger picture, at least not in the past few years. After all, feedback provides useful management information on the use of SARs (a count of feedback received might imply on its own that those SARs were looked at in some way—up to 40 percent of the original disseminations in this case) and their pros and cons. To be fair, feedback received is not always informative, and may say nothing more than "under active investigation or evaluation", an extremely broad category. A cynical view is that LEAs are just providing meaningless feedback to cover their backs (so as to suggest that SARs are being used, when they're not). Since NCIS appears to have carried out little systematic analysis on the feedback received, however, it is not possible to confirm or deny the cynicism. That no systematic analyses have been carried out likely affects the future provision of feedback by LEAs (who might think "if nothing is ever done with information provided, why provide it in the first place?"). More importantly, such systematic analyses repeated at regular (e.g. quarterly) intervals could provide evidence of the use—or not—of SARs by LEAs; if SARs appear to be under-utilised, LEA managers could take immediate steps to improve LEA performance.

79. **Feedback from NCIS to industry**: While not the focus of the research, a brief summary of how NCIS feeds back information to industry is included for completeness. Feedback from NCIS to industry is the province of the Liaison Unit of SFI.[53] The Liaison Unit interacts with industry in three ways: 1) through typology work based on SARs (sanitised and sent to industry); 2) through presentations at industry conferences, often with case examples; and 3) through meetings with the primary industry groups and firms to discuss trends in their SARs (comments received in this research from industry are very positive on these meetings). Interestingly, little of the feedback from LEAs to NCIS is used in the work of the Liaison Unit. NCIS notes that this is because the feedback is largely uninformative—though without any systematic analysis of feedback, this may or may not be the case. Liaison activities have shifted emphasis in the last year from heavy conference attendance to a more focussed approach with industry groups/firms. The Liaison Unit and SFI itself also make use of the *money.web* extranet to provide information to industry and LEAs. *Money.web* provides contact information for LEAs and MLROs, relevant legal documents, discussion groups, and various older short reports on case examples.

80. Very little information is publicly released by NCIS, whether directed at industry or the wider public.[54] Two reports to ministers have been written by the Home Office-coordinated Money Laundering Reporting Task Force (on which NCIS sits), but only as

[53] The NCIS TFT carries out its own liaison activities (in many respects, the TFT operates as a separate entity); these are not discussed here.

[54] In very early discussions with NCIS staff, comments were received which suggested that feedback to industry was to some extent constrained by RIPA: NCIS did not want to be seen as tasking regulated sector entities.

internal documents with restricted readership. NCIS has drafted several documents summarising NCIS SFI priorities and recent changes, but these have been for law enforcement consumption, again with restricted readership (despite the fact that very little sensitive information is contained within and that such documents would likely be of interest to industry). NCIS SFI has suggested recently that it intends to draft and release more information for the public/industry.

81. **Feedback from LEAs directly to industry**: LEAs in many cases provide feedback directly to industry. Much feedback may occur in the course of intelligence development and investigations, as LEAs will be liaising with MLROs for further information. In this sense, much feedback from LEAs to industry resembles liaison as opposed to true outcomes feedback. Specifically, LEAs were asked if they provided feedback directly to industry; just over half of LEAs indicated that this was the case. This is likely an underestimate when thinking of feedback as less-formal liaison or SAR follow-up (many LEAs may have interpreted feedback in the strictest sense). Most feedback, informal liaison or otherwise, does not occur with 100 percent certainty: of the LEAs reporting that they provide direct feedback, nearly fifty percent do so only 20 percent of the time or less. Feedback/liaison appears to provide information to the reporting entity simply on the decision to pursue the matter further or not, though a number of LEAs seem to keep reporting entities in the loop from SAR receipt to eventual outcome. A small number of LEAs noted that feedback/liaison primarily concerns consent SARs, as so few nonconsent SARs were (are) developed/investigated. LEAs indicated that the feedback/liaison process was very useful for relationship-building and to improve industry understanding of law enforcement requirements. Though informal, such feedback/liaison appears well-received by industry, at least as far as LEAs are aware.

82. There appears to be no guidance from any source (e.g. ACPO, Home Office, NCIS) as to whether or not LEAs should be directly providing feedback to industry. Discussions with NCIS personnel suggest that there are concerns, however, that direct feedback may give industry biased viewpoints: what one police LEA considers to be innocent activity, for example, may actually be indicative of complex duty evasion in the eyes of HMCE and/or IR. So reporting entities need to be aware of the possibility that feedback from one LEA may not speak for the true criminality or not behind suspicious activity. These concerns, seemingly valid, have not been shared with LEAs in any formal sense.

5. The System in Flux

83. Finally, the SARs regime is in a state of flux, and has been for some time now. This is largely the result of actions taken by NCIS to improve the functioning of the regime in the long-run. Some factors are worth noting in passing, as they may have had an impact (and may continue to have an impact) on LEA use and management of SARs.

84. **NCIS: The Elmer rollout**: The rollout of the Elmer database on 27 May 2005 is the most positive change within NCIS and the SARs regime. The Elmer rollout will fundamentally change the way LEAs deal with SARs, as the rollout will put access to nearly live data at LEA fingertips. Phase II of the rollout (to be delivered in early 2006) should bring advanced data mining capabilities and numerous other significant enhancements to the system. These include the ability to send automatic notification of

SARs received on selected criteria to relevant LEAs and NCIS/SOCA internally, the ability to bulk download SARs, and enhanced searching on free text data. It seems reasonable that LEAs will be able to launch more proactive investigations with such "young" SARs. And LEAs will be in a position to carry out far more advanced analytical work than at present, at least if they're trained on the system enhancements. But it also places the onus on the use of SARs squarely on LEA shoulders. The SARs-related workload, at least with regard to information evaluation, for each LEA may become overwhelming, as 1) all SARs will be available for viewing by LEAs (save for those related to certain sensitive issues); 2) NCIS will not highlight links to previous SARs; and 3) LEAs will be responsible for all of the various relevant database searches in information evaluation/intelligence development. Resource constraints may prevent certain LEAs from evaluating all of the SARs within their remit/territory. To illustrate, using 2004 as a guide, Table 12, below, presents SARs allocated to each LEA, the LEA percentage of the total number of SARs allocated, the number of SARs allocated per workday (assuming 250 workdays per year), and the number of SARs disseminated per workday. Given comments received on resource constraints with the current SARs workload (which hitherto has been disseminations, not total allocations—which Elmer will emulate), it seems likely that LEAs will feel even more burdened than in the past. Critically, LEAs—particularly the MPS—will need to devise ways to find those SARs which represent a priority. There is most certainly a call for the automation of at least some initial information evaluation, including introducing features within Elmer highlighting links to previous SARs. The one-by-one *manual* evaluation of SARs upon receipt may forcibly become a thing of the past. This is not necessarily an undesirable development, but there will clearly be a need for tools which enable the efficient and effective electronic evaluation of SARs (e.g. keyword searching/advanced data mining). Phase II of the rollout will hopefully assist in this regard. Further, because fewer nonconsent SARs have been disseminated by NCIS since June 2004, LEAs will be facing something akin to a full year's "backlog" of SARs when the database is rolled out. Should these be evaluated (at least in the sense that they're actively looked at one-by-one—they will obviously be very useful in searches of the system and other database interrogation)?[55] Regarding feedback, with the rollout of Elmer, LEAs will be able to easily provide feedback directly to NCIS by pointing-and-clicking their way through an online version of the feedback form. This does not, however, obviate the need for some sort of incentives to greatly increase LEA buy-in to the feedback process. In fact, NCIS will be in a position to monitor use of Elmer, both as an indicator of the use of SARs, and as a means of encouraging LEAs to make regular use of the database (under-performance could be reported to ACPO/LEA managers, who could thus encourage improvements as necessary). Also, should access to Elmer be granted to both FIUs and FIBs (FIBs being the ACPO proposal), there will need to be clear guidelines on which unit will do what, so as to prevent a waste of scarce resources. Regardless of the FIU/FIB decision, LEAs will need to buy into the flagging/ownership of SARs, to prevent wasteful "blue-on-blue" duplication of efforts. Given the paradigm shift in dealing with SARs represented by the rollout of Elmer, there is a strong call for a future review of the regime (including on outcomes), after at least a year of Elmer access by LEAs. The LEA aspects of the regime will clearly undergo considerable change in that time, very likely for the better.

[55] There is some anecdotal evidence suggesting that LEAs appear to be under the impression that they will be expected to work through the "backlog".

Table 12. Annual SARs and Workloads by LEA, 2004

LEA	*2004 SARs allocated*	*LEA percentage of total allocated*	*2004 SARs allocated per workday (estimated)*	*2004 SARs disseminated per workday (estimated)*
Avon & Somerset Constabulary	1,867	1.4%	7.5	0.8
Bedfordshire Police	1,389	1.0%	5.6	0.5
Cambridgeshire Constabulary	1,159	0.9%	4.6	0.7
Cheshire Constabulary	1,279	1.0%	5.1	0.6
City of London Police	695	0.5%	2.8	1.1
Cleveland Police	595	0.4%	2.4	0.3
Cumbria Constabulary	392	0.3%	1.6	0.3
Derbyshire Constabulary	1,043	0.8%	4.2	0.4
Devon & Cornwall Constabulary	1,597	1.2%	6.4	0.6
Dorset Police	1,202	0.9%	4.8	0.4
Durham Constabulary	510	0.4%	2.0	0.4
DWP	889	0.7%	3.6	4.6
Dyfed Powys Police	650	0.5%	2.6	0.3
Essex Police	2,145	1.6%	8.6	0.9
Gloucestershire Constabulary	582	0.4%	2.3	0.3
Greater Manchester Police	5,050	3.8%	20.2	2.1
Gwent Police	586	0.4%	2.3	0.3
Hampshire Constabulary	2,156	1.6%	8.6	0.8
Hertfordshire Constabulary	1,632	1.2%	6.5	0.6
HMCE	6,398	4.8%	25.6	42.3
Humberside Police	968	0.7%	3.9	0.4
Inland Revenue	9,126	6.9%	36.5	38.6
Kent Police	2,042	1.5%	8.2	1.1
Lancashire Constabulary	2,756	2.1%	11.0	1.2
Leicestershire Constabulary	1,681	1.3%	6.7	0.8
Lincolnshire Police	643	0.5%	2.6	0.5
Merseyside Police	1,789	1.3%	7.2	1.0
Metropolitan Police Service	39,150	29.4%	156.6	15.4
NCS	372	0.3%	1.5	1.5
Norfolk Constabulary	925	0.7%	3.7	0.5
North Wales Police	680	0.5%	2.7	0.2
North Yorkshire Police	627	0.5%	2.5	0.5
Northamptonshire Police	844	0.6%	3.4	0.4
Northumbria Police	1,545	1.2%	6.2	0.6
Nottinghamshire Police	1,519	1.1%	6.1	0.6
PSNI	4,125	3.1%	16.5	5.9
SDEA	4,472	3.4%	17.9	3.0
South Wales Police	1,311	1.0%	5.2	0.7
South Yorkshire Police	1,809	1.4%	7.2	1.0
Staffordshire Police	1,287	1.0%	5.1	0.6
Suffolk Constabulary	732	0.5%	2.9	0.4
Surrey Police	3,151	2.4%	12.6	1.1
Sussex Police	2,223	1.7%	8.9	0.9
Thames Valley Police	4,666	3.5%	18.7	1.3
Warwickshire Police	548	0.4%	2.2	0.2
West Mercia Constabulary	1,653	1.2%	6.6	0.7
West Midlands Police	5,985	4.5%	23.9	2.7
West Yorkshire Police	3,709	2.8%	14.8	1.6
Wiltshire Constabulary	979	0.7%	3.9	0.3

Source: NCIS (for allocations and disseminations). 2004 disseminations, on which the 2004 SARs disseminated per workday *column is based, are total disseminations (i.e. original + copied-to disseminations). The* allocated/ disseminated per workday (estimated) *columns assume 250 workdays per year. SARs allocated/disseminated directly to various Scottish forces have been included with the SDEA figures.*

85. **NCIS: The June 2004 reduction of nonconsent disseminations**: In contrast to the positive direction of the Elmer rollout is the unilateral decision taken by NCIS to significantly reduce the dissemination of nonconsent SARs after June 2004 (see page 7 for more detail on the change in procedures). And the issue is not historical in nature: with the Elmer database rolled out, LEAs will need to consider what to do with previously unseen nonconsents (these will be useful in searches and other analytical work based on information interrogation, but should these SARs be evaluated one-by-one, as queried above?). Regardless, there are three issues here: the implications of the June 2004 decision for non-national LEAs (i.e. territorial forces in England & Wales and Northern Ireland, as well as the SDEA, as the point of contact for Scottish forces); the NCIS Service Plan and the aims of the regime; and the manner in which the decision was taken (which relates to ownership of the regime).

86. The main implication of the June 2004 reduction is that few nonconsent SARs have been disseminated to and thus evaluated by *local* law enforcement in almost a year. This would not have been worthy of comment had the Elmer rollout taken place in early autumn 2004 as originally planned. But it did not. As such, according to data provided by NCIS, between July 2004 and April 2005, some 135,633 SARs were received and 15,574 were disseminated; more than 90 percent of these will be nonconsents (see Figure 3, page 52). By these counts, 120,059 SARs have not been seen by LEAs since June 2004, though in actual fact this is an overstatement of the problem. These figures do not take into account the semi-regular bulk CD-based disseminations to Cheshire Constabulary, Merseyside Police, and the MPS. These may represent some 20,000-30,000 nonconsent SARs. So perhaps between 90,000-100,000 SARs will not have been seen by local law enforcement (not all SARs were disseminated to LEAs before the June 2004 reduction, so while this represents a significant change, it is not entirely unprecedented). While these SARs will indeed have undergone considerable keyword and other searches/analyses at NCIS, these searches and analyses have been focussed on *national* priorities as set forth in the NCIS Service Plan. NCIS will generally not have employed keywords relating to *local* targets (i.e. local force priorities, Level One and perhaps Level Two in the NIM). So the concern is that those un-disseminated SARs may hold some important local intelligence which could have prevented crime or at least assisted in its enforcement after-the-fact (though many SARs might be of limited or no value, or relevant only to national issues).

87. To be fair, the present report has highlighted the fact that LEAs were broadly under-utilising SARs; more would not necessarily have improved things (the reduction in nonconsent disseminations may have insulated certain LEAs from criticism). Many LEAs had indicated to NCIS in an internal research effort of the SFI Collections Unit that they were happy to let NCIS filter SARs (i.e. they were happy not to receive all SARs). Actually, filtering was originally recommended by KPMG because LEAs couldn't cope with the volume of SARs they were receiving—but then NCIS was doing at least initial evaluations/examinations of the SARs. And NCIS has suggested that it chose to significantly reduce nonconsent disseminations because LEAs were doing little with the SARs in the first place. Even after June 2004, many LEAs seemed either blissfully unaware that very few nonconsent SARs were coming their way, or knew but didn't object (both discouraging thoughts). Conversations with LEAs suggest that some did welcome the slowdown because they viewed dealing with SARs as competing with other priorities like confiscation and cash seizure. NCIS did provide the LEAs with various workarounds (these were supposed to be temporary, as the Elmer rollout was initially scheduled for

early autumn 2004). These include: LEAs were invited to come to NCIS to use Elmer onsite; LEAs could have filed search requests; NCIS was sending out various subject-of-interest and target lists, all based on SARs; and timely and actionable consent SARs were still being disseminated.

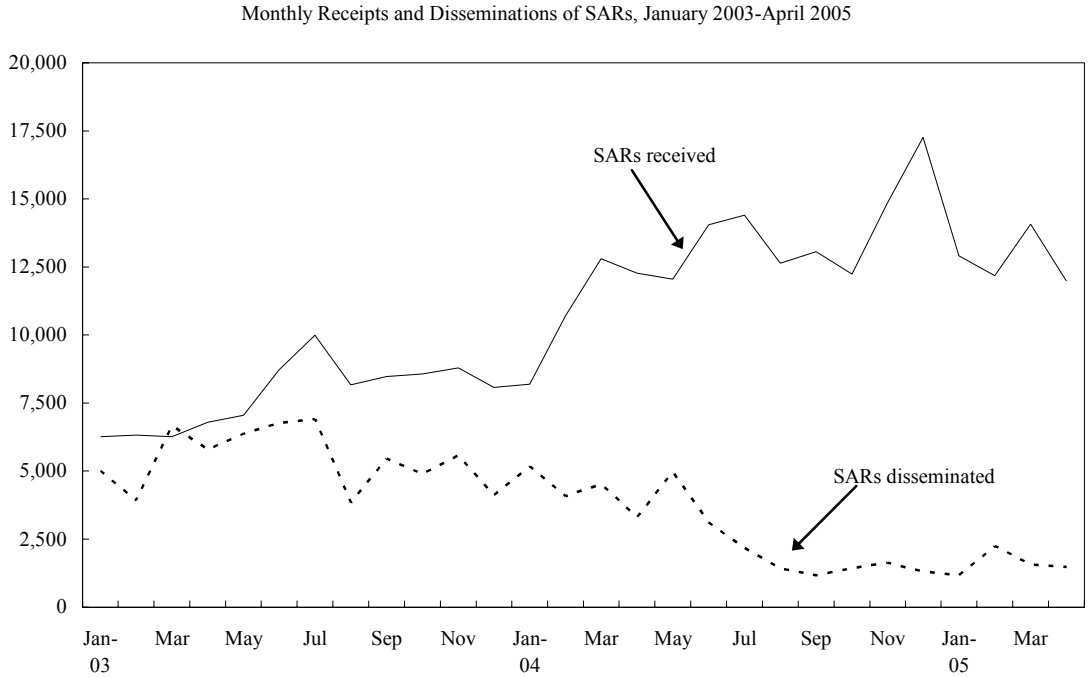
88. But comments received in the course of this research suggest that some LEAs found the workarounds unsuitable (and many of these LEAs represent the larger consumers of SARs). In contrast with those LEAs happy to let NCIS filter SARs, some LEAs wanted to see *all* of the SARs of relevance to them—and this was told to NCIS before the reduction. And not all LEAs were doing little with their SARs; some LEAs appear to have been using SARs to a sufficient and sufficiently interesting extent. A small number of LEAs who might have been underperforming had actually hired staff specifically to deal with SARs, only to find the tap more or less turned off. Moreover, that LEAs were doing little with their SARs seems to be an issue for NCIS to sort out in conjunction with LEA ringmasters at ACPO and the Home Office, not unilaterally. On the work-arounds, very few LEAs seemed to be pleased with the offer to visit NCIS to use the data. LEAs could have filed search requests, but the process is commonly recognised as inefficient and slow (ironically, the results of search requests come through the system as SARs, so an LEA might receive a SAR saying that NCIS has no information to provide for a previously lodged search request). Further, there is some anecdotal evidence that NCIS was somewhat reluctant to conduct vast numbers of search requests to compensate for the lack of nonconsent SARs. After all, it seems that the decision to limit dissemination was inspired by a lack of resources in the first place, and spending untold hours conducting search requests is not drastically different from spending untold hours processing SARs.

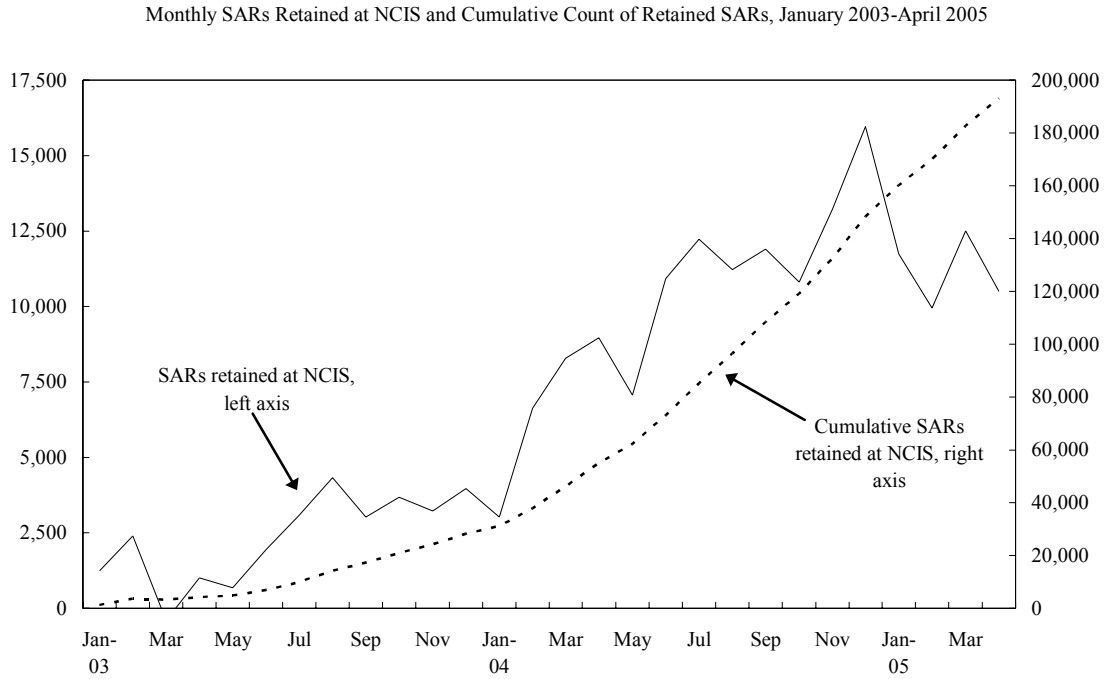
89. In any case, NCIS SFI was not acting in bad faith, of course. SFI was performing the duties and meeting the targets set forth in the NCIS Service Plan. This is the second of the issues relevant to the significant reduction in nonconsent disseminations. Guided by the Service Plan, SFI has recently focussed on supporting national strategies (CICFA, CIDA, REFLEX, firearms), which is reasonable—and some of this work is very exciting. What is not as reasonable, however, is that this focus may have been partly at the expense of local LEAs, who also have a role to play on SARs. What, then, are the overall aims of the regime? Are they to combat national-level serious and organised crime, or are they to combat local priorities (Level 1 of the NIM), or <u>both</u>? The regime appears to not have any governing mission statement which clarifies this in any way (or at least one agreed by all relevant parties). The Service Plan objectives seem to support the role of SARs nearly exclusively in national-level crime-fighting, but perhaps only because the issue has never been fully raised and resolved. The Service Plan appears too narrowly focussed, failing to explicitly recognise the potential for SARs to contribute to local strategies (in this regard, the SARs regime represents an anomaly for NCIS, which otherwise focuses exclusively on national serious and organised crime). NCIS does, in fact, assist local law enforcement through the Elmer rollout. But this was largely not the case for one year of the regime's history. With different—and explicit—aims for the regime driving a different Service Plan, it's unlikely that the reduction in nonconsents would have taken place in the way that it did. The aims of the regime must be made explicit.

90. Lastly, there may have been some considerable ramifications of the June 2004 decision that deserved greater discussion and perhaps approval within and from the larger SARs community. This raises the third issue, the manner in which the decision was taken—and ownership. By all accounts, the communication on the decision was poor. Regional NCIS offices were not aware of the June 2004 reduction until weeks or in some cases months later. LEAs were not informed. Industry was not informed. Some claims have been made that discussions around the issue were held in high-level meetings, like with CICFA and the MLRTF. If this is the case, meeting attendees don't seem to have been fully aware of the implications of the discussion. Clearly, the ramifications of the June 2004 decision do not appear to have been fully thought through. Was the decision made with seemingly little forethought because of a perceived lack of accountability? This may be the case because the regime has no owner. Such weighty decisions should probably take place with greater concern for all parties involved, guided by firm ownership.

91. **HMRC and SOCA**: Finally, two sizable mergers are worthy of attention in the criminal justice system. Inland Revenue and HMCE became Her Majesty's Revenue and Customs on 18 April 2005, and, of more direct relevance to the SARs regime, NCIS, the National Crime Squad, and certain investigative units of HMCE are merging to become the Serious Organised Crime Agency (expected in April 2006). This implies that SARs will be disclosed to SOCA; NCIS will no longer exist. Details surrounding the impact of the merger(s) on the regime have yet to be discussed. Two points are worth making on the SOCA setup; 1) it is essential that the regime—which should by no means only focused on the most serious of offenders—does not get lost in the shuffle; and 2) critically, the formation of SOCA presents a rare window of opportunity to right many of the wrongs of the past in one fell swoop.

Figure 3. Monthly Receipts and Disseminations of SARs by NCIS, January 2003-April 2005





Source: NCIS. Disseminated SARs include LEA-bound consents but exclude SARs related to terrorism and various other sensitive issues; SARs destined for overseas jurisdictions; SARs sent out in bulk backlog-clearing exercises (see footnote 45); and SARs sent to NCIS units other than SFI. According to these figures, roughly 120,000 SARs were retained at NCIS between July 2004 and April 2005. But some 20,000-30,000 SARs will have been disseminated via CD-ROM to several LEAs, so the true number retained at NCIS is perhaps between 90,000-100,000. These will have been subject to national-level (but generally not local-level--and this is the issue) keyword searches/other analyses. As at June 2005, retained SARs are available to LEAs via the rolled-out Elmer database.

B. The Experiences of Overseas Jurisdictions

92. This research, as noted, is driven in large part by the desire of regulated sector entities for systematic information/feedback, for reassurance that their efforts are rewarded by sufficient appropriate action on the part of law enforcement. Of course, such reassurance is not forthcoming at present, seemingly due at least as much to limitations in information management as to whether or not SARs are actually being used. A number of recommendations for improvement(s) to the regime with regard to systematic information and feedback simply fall out of a deeper understanding of LEA protocols and policies. But another potential source of insight is the experience of overseas jurisdictions, who may have faced similar issues in their own countries. As such, the research looked to a small number of national financial intelligence units for their specific thoughts. Given the short timeframe of the study, efforts were focussed on three such units: the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Financial Crimes Enforcement Network of the United States (FinCEN), and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Among other things, the three were asked whether they had faced such concerns of industry, namely perceptions that little is being done with the reports provided and/or that perhaps SARs (or similar reports) are of little crime-reduction value; and what solutions were implemented to address such concerns.[56] Conversations held with parties from outside these units and a search of the (limited) relevant literature rounded out the analysis. International findings are summarised below.

93. By way of background, each of the three national financial intelligence units is a stand-alone organisation. AUSTRAC sits under the Australian Attorney General's Department, FinCEN sits under the US Department of the Treasury, and FINTRAC sits under the Department of Finance Canada.[57] Each unit is responsible for the receipt and analysis of raw SARs and other financial transaction reports (FTRs; all three receive both suspicion- and threshold-based reports).[58] Each unit states that all SARs are evaluated, though in the case of FinCEN, this appears to happen in conjunction with law enforcement (through what are known as High-Intensity Financial Crime Areas, or HIFCAs). Unlike NCIS, each unit also has regulatory oversight of its AML regime. This implies that while the units make use of the information provided by the reporting entities, they also liaise directly with these entities with both carrots and sticks to ensure compliance with AML regulations (i.e. to ensure that the information provided is timely, accurate, and high-

[56] The research recognises that national financial intelligence units do not control the use made by LEAs of financial information/intelligence and do not speak on their behalf. But they should be aware of the lay of the land. Time limitations prevented deeper research with foreign LEAs directly.

[57] This section is not intended to provide a complete exposé of the roles and responsibilities of each national financial intelligence unit. For detailed information, see each unit's annual report: AUSTRAC (2004), FinCEN (2005), and FINTRAC (2004), all available online. For more on the various functions of national financial intelligence units around the world, see IMF/WB (2004) and Thony (1996). Gold and Levi (1994), KPMG (2003), and PIU (2000) also present some limited comparative international information, though not on the topics discussed here.

[58] Note that each unit deals with suspicion-based reports (referred to by AUSTRAC, FinCEN, and FINTRAC as SUSTRs, SARs, and STRs, respectively) as well as various types of threshold-based and other reports; suspicion-based reports and other financial transaction reports will be referred to as SARs and FTRs for the purposes of this section.

quality).[59] None of the units has an operational arm, so, like NCIS, SARs/FTRs and/or other intelligence products are sent to various LEAs for action. All units provide LEAs with enhanced tactical (and, increasingly, strategic) intelligence products, which are the results of data-mining, cross-referencing other databases, and/or other analytical exercises. AUSTRAC and FinCEN (but not FINTRAC) provide select LEAs with remote electronic access to their raw data in arrangements governed by various legal gateways and MOUs; access levels may differ according to the security clearance levels of registered users. Search requests may also be filed by interested LEAs to AUSTRAC and FinCEN; search requests are prohibited under Canadian legislation, though LEAs may submit "voluntary information" alerting FINTRAC to their current operational priorities (FINTRAC may then make use of voluntary information to tee off intelligence development).[60] Statistics on the number of SARs/FTRs received by each unit, as well as by NCIS, are presented in Table 13, below.

94. What, then, of the experiences of the three financial intelligence units? Most importantly, each of the units noted that systematic feedback on the LEA use of SARs (and other FTRs) is lacking, as in the UK.[61] In fact, each somehow acknowledges the issue and its importance in various publicly-available documents, such as annual reports and speech transcripts. Other public bodies have occasionally weighed in (e.g. Auditor General of Canada, 2004). The limited provision of systematic LEA feedback prevails for the traditional, perhaps universal, reasons discussed earlier in the present report (see page 17), including: operational priorities may preclude the reporting of feedback (or at least timely feedback); the period of time between the use of SARs/FTRs and case outcomes may be so large that details (or the importance of feedback) are forgotten; the initial users of SARs/FTRs may differ from those ultimately responsible for the case outcomes (with little cross-talk between the groups); and limited IT systems and protocols may render the provision of feedback difficult or impossible.[62]

---

[59] FinCEN does not actually conduct the compliance examinations; these are carried out by regulators of the specific industries involved.

[60] Legislation prohibits FINTRAC from disseminating the complete results of its analyses to LEAs; rather, *disclosures* (as they're known) contain the who, what, when, where, and little else. LEAs may gain access to full analyses via a court order requiring FINTRAC to produce relevant information, though this avenue has not been widely used.

[61] That little is known about the LEA use of SARs and their threshold-based brethren comes as no surprise. While the literature is thin, of the few and sometimes dated non-UK sources, most conclude that insufficient information exists on the actual use of SARs/etc. The most comprehensive analysis is that of Reuter and Truman in their 2004 analysis of the global AML regime. They focus heavily on the situation in the US, noting that "for the 6½ year period ending October 3, 2002, 940,000 SARs produced 70,000 direct referrals to federal law enforcement agencies, of which almost half were to the FBI. Unfortunately, there is no information on how many resulted in or contributed to cases". Another example is van Duyne and de Miranda (1999), who find for the Netherlands that "hardly anything is known [in their own research] as to what the follow-up measures of the police and prosecution might have been, owing to a lack of feedback from the 'field'".

[62] Feedback from LEAs on the use made of SARs may also be lacking because the information provided by financial intelligence units is infrequently used. Reuter and Truman (2004) found some evidence in the US that "the existing regulatory system and the information it generates is not well used in prosecutions". The Auditor General of Canada highlighted the fact that the value to LEAs of FINTRAC's disclosures

(continued)

Table 13. SARs/FTRs in Australia, Canada, the United Kingdom, and the United States

Country	*2000*	*2001*	*2002*	*2003*	*2004*
			SARs received		
Australia	7,068	7,247	7,809	8,054	11,484
Canada	--	--	3,772	17,358	14,794
United Kingdom	18,447	29,976	56,023	94,708	154,536
United States	163,184	204,915	281,373	506,948	639,884
			SARs received per population millions		
Australia	369.0	374.5	399.6	408.2	576.3
Canada	--	--	120.6	550.9	465.8
United Kingdom	314.3	509.1	948.4	1,598.4	2,599.9
United States	572.6	711.4	966.8	1,724.1	2,154.1
			SARs received per unit of GDP (US$ billions, current prices)		
Australia	18.7	20.3	19.5	15.7	18.6
Canada	--	--	5.1	19.9	14.9
United Kingdom	12.8	20.9	35.7	52.6	72.7
United States	16.6	20.2	26.8	46.1	54.5
			FTRs received (aggregate figures for all non-SARs reports)		
Australia	7,052,190	7,815,416	8,937,426	9,501,485	10,768,039
Canada	--	--	--	2,086,153	9,482,536
United Kingdom	--	--	--	--	--
United States	13,416,587	12,996,620	13,105,206	13,286,257	13,751,730

Sources: AUSTRAC (2004), FinCEN (2004a; 2004 SARs figure estimated from January-June 2004 data), FINTRAC (2004), and NCIS; IMF World Economic Outlook database, April 2005 revision (for GDP); IMF International Financial Statistics database (for population; 2004 figures estimated from 2000-03). FINTRAC was operationally launched in 2001, so no data are available prior to 2002. Figures from AUSTRAC and FINTRAC were provided in fiscal year format, such that 2004 data represent information for 2003-04. Also, AUSTRAC and FINTRAC officially refer to their SARs as SUSTRs and STRs, respectively. FTR figures for AUSTRAC include SCTRs, IFTIs, and ICTRs; for FinCEN figures include CTRs, CTR-Cs, and 8300s; and for FINTRAC figures include LCTRs and EFTRs. The UK does not use FTRs.

95. This is not to imply that no feedback is ever received from LEAs, however. On the contrary, at least in Australia and the US, while levels of systematic feedback appear to some extent suboptimal, both jurisdictions seem to fare somewhat better than the UK. (Canada's system, launched in 2001, is so new that priorities were reasonably focussed on getting the system up and running, ensuring the smooth functioning of its electronic reporting systems through to the successful disclosure of information to LEAs. Improving the systematic understanding of the use by law enforcement of FINTRAC disclosures is

(containing only the "designated information" permitted by legislation) was limited by the lack of detail and context in the disclosures themselves (Auditor General, 2004).

now becoming a priority.[63] Anecdotal evidence suggests that LEAs find the disclosures of value.) Interestingly, in the MOUs agreed between AUSTRAC and its law enforcement partners allowing access to AUSTRAC information, AUSTRAC requires LEAs to provide feedback on a quarterly basis (including on the remote use of databases). LEAs generally comply, according to AUSTRAC. AUSTRAC and FinCEN include brief feedback questionnaires with various intelligence packages they send out, though with admittedly imperfect response rates (e.g. FinCEN reports a 50 percent response rate). Relations with LEA partners appear strong. In this regard, AUSTRAC and FINTRAC have outposted liaison staff (AUSTRAC staff are outposted with LEAs; FINTRAC staff are outposted in FINTRAC regional offices), and FinCEN reports that most federal agencies have liaison staff of their own posted at FinCEN. Liaison staff provide channels for ad hoc feedback. Moreover, these liaison staff may have responsibilities which include the collection and provision of feedback back to the financial intelligence unit (e.g. AUSTRAC staff may suggest procedures to increase the efficiency and effectiveness of feedback, or they may follow-up with the partner agency to clarify information on investigations where they know that SARs/FTRs have been of use). Liaison staff may also provide analytical training and support to partner agencies.

96. Encouraging the use of SARs/FTRs and encouraging feedback is a never-ending part of the workload of each unit. All of the units appear to maintain ongoing training programs for LEAs on the importance and potential of financial intelligence, and the feedback issue is raised repeatedly. But beyond such routine activity, each unit is taking or has recently taken active steps to improve the systematic understanding of the use of financial reports and intelligence. AUSTRAC, for example, employed a consultant to explore the limitations in feedback systems and to suggest improvements (e.g. through standardising feedback processes, through initiatives to educate LEAs on why feedback is needed, through the use of staff with direct responsibility for the provision of feedback, through the use of case management systems). FinCEN is awaiting the completion of *BSA Direct*, its new information storage and delivery system (pulling together reporting entities, FinCEN, and LEAs). Among the many stated benefits of the system is an improvement of feedback to industry.

97. Finally, and moreover, concerns that systematic feedback on the LEA use of SARs is lacking should be viewed in the context of information provided to the public directly by AUSTRAC, FinCEN, and FINTRAC on developments in their AML regimes. In stark contrast to the UK, the three units provide a wealth of information to the public, primarily (and most efficiently) through their websites. All publish an annual report as well as various other documents, including transcripts of speeches, guidelines and guidance notes, newsletters, biannual reviews, information circulars, and strategies for the future.[64] AUSTRAC is the first of the units to launch an online e-learning initiative to assist in the education/training of the regulated sector and public-at-large. Most publications discuss

[63] FINTRAC potentially faces a less-daunting task: FINTRAC releases fewer than 200 of its disclosures (which are not individual reports, but rather enhanced intelligence products) to LEAs per year. The average disclosure relates to three million Canadian dollars, with five individuals and three business involved, relating to some 57 transactions from three reporting entities (FINTRAC, 2004).

[64] NCIS SFI publishes no publicly available report (and the NCIS *Annual Report* mentions SARs in far too much generality to be of use).

the use made of SARs/FTRs by LEAs, including statistics on trends and case examples. This information may be drawn from the internal monitoring of database access (e.g. through metadata on the numbers of logins or searches), from the above-mentioned semi-regular feedback from LEAs, or from one-off conversations regarding specific cases (FinCEN, for example, reaches out informally to LEAs three times each year for case examples for the *SAR Activity Review*). Publications typically are designed with reporting entity input, and are often sent to select industry representatives/groups for comment/review prior to publication. Industry seems to hold the publicly available information of the three units in high regard. In fact, relations with industry in the three jurisdictions appear broadly healthy and positive. Each unit has a sizable outreach/liaison program with industry, not least given the regulatory functions that each must carry out. FINTRAC spent considerable time with reporting entities preparing for its operational launch in 2001. AUSTRAC, in particular, appears to have a strongly cooperative relationship with reporting entities, thought to be the result of a long-standing focus on carrots—not sticks—in its regulatory approach, as well as continued emphasis on training materials.[65] Like the UK, Australia and the US maintain permanent advisory groups with government, law enforcement, and industry membership (AUSTRAC's Provider Advisory Group and FinCEN's Bank Secrecy Act Advisory Group), which discuss AML policy and relevant issues, like policy design, feedback and publications.

98. In sum, while each of the three units receives suboptimal amounts of feedback from LEAs on the use made of SARs/FTRs and related intelligence packages, performance relative to the UK in this regard appears superior. According to the units, whilst reporting entities had registered concerns that feedback could be improved, entities in general did not seem to feel that their reports were unused or of little value.[66] In large part, this appears to be the result of 1) an abundance of publicly available information drawing on moderate amounts of feedback on the use of financial reports; and 2) good liaison between AUSTRAC, FinCEN, and FINTRAC and their law enforcement partners, and with industry itself; 3) efforts to obtain feedback from LEAs (e.g. through active feedback-gathering efforts on the part of liaison or other staff, through steps taken to streamline and improve feedback processes, and through ongoing training activities).

---

[65] While in no way suggesting that sanctions should never be used in enforcing regulatory violations, there is an unavoidable downside (particularly when sanctions receive press coverage): an increase in defensive reporting. This appears to be an issue at present in the US, following highly visible actions taken against Riggs Bank and Amsouth Bank.

[66] This is confirmed by industry comments received from various foreign sources which suggest that reporting entities do not feel that the information they provide is unused, but rather that 1) there is an imbalance between their efforts and those of government, including LEAs (not least given industry outlays on systems/training/staff); and 2) that the information is not used as effectively or efficiently as it could be (e.g. *how are SARs prioritised?* and *what sort of advanced analysis/datamining is carried out?*).

C. The Regulated Sector and Its Desires for Feedback

99. But what of the regulated sector? *What are LEAs doing with SARs?* is a valid question. But so is *what does the regulated sector expect LEAs to do with SARs?*, as is *what sort of systematic feedback does industry really want?*. Given that this research has been partly motivated by regulated sector calls for information/feedback, it seemed appropriate to actually turn to the regulated sector in the UK to determine its wants and needs. Time prevented an extensive industry-wide call for comments; instead, the primary oversight bodies of regulated sector entities were unofficially canvassed for their input. Through the Treasury, a questionnaire was sent to the relevant anti-money laundering contact in each industry organisation within the Money Laundering Advisory Committee (MLAC); 27 responses were received.[67] Information obtained through the questionnaire was complemented by personal interviews with select industry members. Findings are presented in the pages that follow; the questions placed to industry are presented in italics, followed by a summary of their responses (interview comments are worked into the text as appropriate).[68]

100. Are you satisfied at present with the feedback you receive from NCIS, LEAs, and government? Respondents were almost universally dissatisfied with feedback. Many respondents noted that they received little if any feedback at all. A few respondents indicated that they received occasional feedback from local police, and several specifically mentioned visitations from NCIS in a positive light, but all in all feedback appears lacking. One respondent pointed out that much of the feedback was too sanitised to be of any use (or it simply told him/her what he/she already knew); the only useful feedback was that received informally. Another respondent suggested that feedback was simply not a priority in NCIS, a fact which was viewed as unacceptable. Yet another wondered what had happened to the *source of feedback* letters, which had "ceased without explanation" *(these at one point were used to indicate the usefulness of SARs on a case-by-case basis).*

101. *What sort of systematic feedback do you want to see? That is, what do you really want to know from NCIS/LEAs?* This, of course, is the crux of the issue. Respondents were quite detailed in their responses. Respondents generally want to receive information on receipts of SARs by NCIS; dissemination of SARs to LEAs; typologies; general information; and information to improve reporting. A compilation of responses is presented in Table 14, below.

102. *How would you like feedback to be presented (e.g. in a hard-copy published report, posted online, verbally)?* Perhaps not surprisingly, the majority of respondents felt that feedback posted online was the optimum, though a good number seemed to suggest that it was important to have a published report. Many respondents were not interested in the medium, just the message: as long as some sort of feedback product was put together, how it was delivered was secondary. A few respondents suggested that filer-specific

---

[67] Certain MLAC members further sent the questionnaire on to constituents for comment. Respondents primarily represent industry bodies (e.g. BBA, Law Society) or some of the largest of the reporting entities.

[68] KPMG (2003) also explored regulated sector wants/needs. Despite being some two years ago now, similar themes emerge.

feedback from NCIS or LEAs would be best in hard copy or in person, particularly anything sensitive (e.g. information relating to the quality of the reports filed, to an ongoing inquiry, or regarding the specific uses of their own SARs). A number of respondents stated that they felt that live presentations (e.g. workshops with larger institutions, or conference presentations with industry groups) were useful; and that newsletters could convey less-official and more timely information.

Table 14. What Sort of Systematic Feedback Does the Regulated Sector Want to See: A Compilation of Responses

Feedback
Receipts of SARs by NCIS
Total numbers of reports filed by sector and by month
Total numbers of consent requests filed by sector and by month, including:
Percent granted within the 7 days
Percent refused within the 7 days
Percent resulting in assets being restrained and amounts restrained
Average and longest/shortest time for response
Categories of criminality identified from SARs
SARs disseminated to LEAs for action
Number of SARs forwarded to LEAs for action
Number of SARs that contributed to ongoing investigations (and numbers of those leading to a court order)
Number of SARs that initiated investigations (and numbers of those leading to a court order)
Number of cases resulting in successful arrests, prosecutions, cash seizures, confiscations
Figures for cash and assets recovered, divided into:
Those where there was no SAR impact
Those where a SAR may have contributed
Those initiated by SARs
Number of SARs that were of no intelligence value—with feedback on how these could be improved (any feedback should distinguish between fraud and money laundering to avoid confusion on those which are mandatory, i.e. reports on fraud that has been committed)
Geographic areas (postal codes not force boundaries) that SARs have been referred to and types of prominent criminality within that area
Specific type of criminality reported by a particular sector (i.e. carousel fraud by retail banking sector)
Typologies
New money laundering techniques
Current trends within existing techniques
Identification of more prominent typologies
General information
Number of financial investigators by LEA
Annual summary of the importance of money laundering within the National Policing Plan
Information to improve reporting
On a one-to-one level, some feedback from LEAs who have communicated with industry after submission of a report (e.g. to get production orders) as to what happened
Number of SARs which were "rejected" as of being of little or no value or where they believe that no crime has been committed
Examples of SARs that were of use and those that were a waste of time
Regular examples of good and poor practice in reporting
Feedback to each institution on the quality and usefulness of the SARs they submitted

Source: Various regulated sector respondents.

103. *With what frequency would you like to receive feedback (e.g. annually)?* Though the odd request was made for monthly feedback, most respondents suggested that annual or biannual feedback would be appropriate. A number of respondents spoke of the desire for some form of annual product, supplemented by detailed quarterly/biannual output (e.g. on industry-specific statistics, on the quality of reporting). There were several calls for higher-frequency feedback on specific issues—like ongoing cases and/or emerging trends/typologies—though there was a tacit recognition in some comments that this would be unlikely given resource constraints.

104. *From whom exactly would you like to receive feedback (directly from LEAs, or routed through NCIS or perhaps even the Home Office)?* Respondents were fairly unanimous in claiming that feedback should emanate from NCIS. Many respondents reported that they would like direct feedback from LEAs, though even this could be routed through NCIS for consistency. A number of respondents didn't seem to care where the information came from, as long as it was official, regular, and authoritative—and delivered in an efficient and effective manner. The occasional respondent noted that different kinds of feedback should come from different sources, with NCIS providing the bulk of information relating to disclosures, for example, and the Home Office providing information on the efficacy of the AML regime.

105. *Why do you want feedback (or if you don't care about feedback, why not)?* Respondents typically cited four primary reasons supporting their desire for the provision of feedback: feedback allows reporting entities to improve the quality and completeness of their SARs; feedback allows industry to better understand the needs of NCIS/LEAs (allowing for better targeting of suspicious activity, through training or the modification of detection systems, potentially reducing the number of SARs filed); feedback illustrates the crime reduction efficacy of the regime ("useful to know if our huge effort in time + cost is actually having any effect on combating crime"); and feedback provides tangible evidence of the use of SARs to those making resource allocation decisions within reporting sector firms. On this last point, one respondent put it this way: "executive boards like the regime, but they don't like unfocussed cost with little discernible benefit". Certain respondents suggested that they wanted feedback because it acted as an accountability mechanism for NCIS/LEAs who might otherwise under-perform on SARs. And several respondents noted that it was simply reasonable to want to receive feedback given their outlay on compliance with the SARs regime.

106. *What do you expect LEAs to do with SARs (e.g. should they fully investigate each SAR)?* Despite a public perception that reporting entities expect LEAs to fully investigate each and every SAR, most respondents appeared to hold a more nuanced view that the SARs should be subject to some prioritisation; those deemed to have higher priority should then be investigated, subject to resource constraints. A few respondents suggested that the system was based on cumulative information, and that SARs should be investigated when they cumulatively begin to indicate criminality—save for those SARs sufficiently compelling on their own to call for investigation. Several respondents did, however, suggest that *all* SARs should undergo some sort of cursory evaluation upon receipt so as to allow for prioritisation. Ideally, then, some information could (and should, several opined) be maintained on each SAR about identified links to criminality and SAR quality. This information could subsequently be used for the production of feedback/ statistics. A small number of respondents noted that they expected LEAs to at least have

access to the information—SARs themselves and relevant attachments. And there was a sense captured in one response, though reflected throughout the responses to most of the questions put to industry, that the regulated sector expected LEAs to effectively utilise SARs "if the entire basis of current legislation and regulation is not to be undermined".

107. *Do you perceive SARs to be under-utilised, over-utilised, or correctly-utilised by LEAs? What makes you say this?* Respondents reported with near unanimity that the perception was that SARs were under-utilised by LEAs. One respondent even suggested that low-value intelligence reports probably weren't being used at all. One positive view was from a respondent noting that the use of consent SARs appeared to be on the increase. The basis for judgment was often the lack of feedback itself. And some (presumably larger) reporting entities noted that the volume of production orders as compared to disclosures suggested that only a very small proportion of SARs resulted in or involved an investigation (although in one case this was noted to be 20 percent, which may not be so low). A small number of respondents maintained that they couldn't comment on utilisation (despite the fact that the question was exploring *perception*, not fact), as they had so little feedback that they didn't know how/if SARs were being used. Most indicated a belief that LEAs and NCIS were not sufficiently resourced to do the job (of great consternation to industry as a whole, given its considerable AML expenditures), not least with the massive increase in reporting, much of it defensive. Interestingly, several respondents interpreted the question as relating to industry, and suggested that industry was over-utilising (i.e. over-reporting) SARs in a defensive posture to prevent being prosecuted themselves.

108. *What would you consider to be evidence of the crime-reduction value of SARs?* While many respondents weren't sure what they would consider as evidence of the crime-reduction value of SARs—this is an academic issue, and a complex one at that—several indicators were highlighted. These reinforced what was described in the question on the sort of feedback industry was looking to receive. These included quantitative and qualitative measures of SARs-related prosecutions/convictions, production orders, assets recovered, and press coverage. It probably comes as no surprise that these indicators mirror those suggested by the FATF and others. For one, MLROs and other SARs-related industry types are typically well-read on all things SARs, and will likely be familiar with the FATF recommendations on statistics and its assessment methodologies. But this is also about common sense: these are the things that people naturally think of when discussing the impact of AML policies (excluding the ever-critical deterrence, of course).

109. *Additional comments*: Regulated sector entities were also given a chance to provide any additional comments. One respondent noted that while it was easy to criticise the regime, significant steps had been taken in the last decade in the regulated sector's efforts to assist in the fight against crime. Another called for more research on both the impact of AML legislation and the cost implications of AML policy (specifically if the costs and benefits were proportionate). Yet another suggested that many of the reporting entities recognised that money laundering often involves complex financial products/procedures, which industry was willing to help law enforcement to understand—but then, given this offer of assistance, law enforcement must not turn around and say that some things are too complex to investigate. Finally, some participants in the exercise called for the high-level vetting of a number of appropriate industry individuals who could be given sensitive feedback and typologies, and who could play a much more coordinated role with the criminal (and national security) intelligence community. This seems to be an eminently sensible proposal, though it doesn't obviate the need for the provision of worthwhile feedback from LEAs to NCIS.

V. DISCUSSION AND RECOMMENDATIONS

110. So are SARs currently being used by LEAs? What sort of contribution do they seem to be making to crime reduction? What can be done, particularly to the way in which LEAs manage SARs, to increase the likelihood that law enforcement, policy-makers, and industry can make informed judgments about SARs' contribution to crime reduction? This chapter discusses the implications of the research and presents recommendations for action. Note that any recommendations which concern NCIS should apply in the future to SOCA.

111. **Despite evidence of some important SARs-related successes, the central finding of the research is that SARs appear to be under-utilised by most LEAs**. This is not to suggest that *all* LEAs are under-performing on SARs; a number of LEAs appear to be carrying out some good work with SARs (both proactive and reactive). Some examples are contained in Appendix 1; others are of interest but remain *sub judicae* (and out of the public domain); and still others are of interest but relate to cases in which the use of one or more SARs has not been made public. Moreover, all LEAs appear to do at least *something* with SARs.[69] But the available data—admittedly of low quality and limited depth—*coupled with the admissions of LEAs themselves* together suggest that SARs could be better and more frequently utilised. Why is this the case? A number of factors were identified which appear to contribute to this under-utilisation, including the following (though not all will be relevant for each and every LEA):

- **LEAs appear to have insufficient resources** to develop and exploit the information contained in SARs.
- **SARs-development units (typically FIUs) often view confiscation and cash seizure as competing with SARs for scarce resources** (even though the work is very likely complementary).
- **SARs-based cases are difficult to sell to operational teams** (perhaps in part because tasking and coordinating groups are reluctant to assign scarce resources to jobs based on little more than one or many reports of suspicion, not established criminality).
- **IT systems commonly used allow for only limited SARs-related analyses** (this is even more relevant with SARs management approaches which rely on hard-copy files only). The rollout of Elmer to some extent addresses this; Phase II of the rollout in particular will provide much more advanced analytical capabilities.
- **SARs may contain unclear reasons for suspicion or may relate to noncriminal activity** (i.e. disclosures may be incomplete and/or represent mistaken suspicion or purely defensive reporting).

[69] Word around the campfire at the onset of the project had suggested that certain LEAs were doing nothing with nonconsent SARs (e.g. placing them unused in office files). This behaviour could not be confirmed. That this may have been the case historically cannot be ruled out, however.

- **LEAs receive little guidance/training/advice on the use of SARs** (e.g. in turning confidential information into usable intelligence, data mining, best practice, and minimum work required).

- **Few carrots or sticks drive the use of SARs**: no performance indicators encourage LEAs to make proactive/reactive use of SARs (and only things which are measured appear to get done).

- Along these lines, **there is no larger accountability for either LEAs or NCIS on the use of SARs; the regime has no real owner to encourage solid performance, to effect change, and to coordinate the SARs-related activity of numerous government departments and agencies**. **Neither is there a mission statement which clearly sets out the aims of the regime**.

112. **Furthermore, systematic information maintained by LEAs on their use of SARs is limited and often of poor quality**. This appears to be the case because:

- **LEAs employ limited if any case management systems or approaches** (or if such systems are employed, limited IT fluency prevents statistics from being produced).

- **Insufficient LEA resources limit the availability of systematic management information**. Such resources include intelligence developers, financial investigators, or even clerical support.

- **Many LEAs claim to be unaware of the statistical indicators which might be of interest to industry and the larger policy community**. These LEAs state that they would be happy to provide systematic information on the use of SARs; they just need to be told what data to keep.

- And **some LEAs may exhibit a disdain for record-keeping**.

113. Some systematic information on the use of SARs is, of course, maintained by LEAs. **But this information—particularly the feedback provided to NCIS—is under-utilised by NCIS and subsequently by industry and the larger policy community**. NCIS has done little in the way of *systematic* analyses of LEA feedback (it is unclear why this is the case). Certain LEAs may maintain quality usable feedback on SARs, which could assist industry and guide policy decisions—or maybe not, but the only way to find out is to perform systematic analyses, not simply occasional checks of the odd feedback form. A lack of systematic analyses of feedback, if not addressed, may ultimately serve as a disincentive to LEAs who need to improve their feedback, not cut back on it. Systematic analyses of feedback could (and should) be used to inform ACPO/LEA managers on LEA use of SARs.

114. **Communication and feedback between and within LEAs, NCIS, ACPO, government, and industry is suboptimal**. For example, industry appears dissatisfied with feedback provided from official sources (especially NCIS, whom reporting entities feel should channel feedback from LEAs and NCIS itself to industry). There is no annual report for the regime (which could/should among other things describe LEA use of SARs), and limited guidance is provided to the regulated sector. This is in stark contrast to the situation in Australia, Canada and the US: AUSTRAC, FINTRAC, and FinCEN all

provide considerable information to industry and the broader public, primarily through their websites. Further, communication and relations between LEAs and NCIS are poor. This manifests itself, for example, with intelligence products, which the LEAs do not seem to have received with any great frequency. This may be by design; intelligence products are often released on a need-to-know basis. But NCIS and LEAs should ensure that their communications channels are open and effective, not least if NCIS is using scarce resources to provide SARs-based intelligence products to LEAs who don't seem to receive and/or use them. And it seems unclear to LEAs what is expected of them with regard to SARs, suggesting not only that training/guidance/advice is insufficient, but also that there is a strategic disconnect between LEAs, ACPO, government, and perhaps NCIS. While numerous reasons explain the suboptimal communication, it seems likely that the lack of accountability and the lack of an owner of the regime are most significant.

115. **On a positive note, change is afoot in the SARs regime—especially with the rollout of the Elmer database and the creation of SOCA**. The rollout of the Elmer database to LEAs nationwide represents a tectonic shift in the manner in which LEAs deal with SARs. It will greatly facilitate the use of SARs, particularly with Phase II of the rollout (what with its advanced data mining capabilities, bulk downloading, etc.). But it will also place the onus of using SARs squarely on the shoulders of LEAs. And it will not relieve NCIS of all burdens: NCIS will still need to maintain the database, to deal with the timely inputting of SARs, and to consider the wants and needs of LEAs as users of SARs (in addition to developing any tactical or strategic SARs-related intelligence products). On SOCA: the creation of SOCA, as a break from the past, presents a rare opportunity to right many of the wrongs of the regime in one fell swoop.

116. So what can and should be done to fix LEA-related aspects of the regime? **Fifteen recommendations fall from the research**. All should improve LEA use and management of SARs and should allow for systematic information to be captured by LEAs, assembled by NCIS, and consumed by industry and policy-makers.[70] Recommendations are classified as *critical*, *highly desirable*, and *desirable*.

117. Recommendations are as follows:

118. **Recommendation 1 (critical). For accountability purposes and to coordinate the activities of the various relevant government departments and agencies, the SARs regime should once and for all be assigned an "owner" (most likely NCIS/SOCA with a slightly expanded remit), and this owner should be governed by an oversight board**. This is very likely the most important recommendation in the long run. The lack of accountability of all/most parties in the regime is striking: shouldn't ACPO be held accountable for the under-utilisation of SARs by police LEAs? Shouldn't the LEAs themselves, ACPO, NCIS, the Home Office, and HMT be held accountable for the fact that few LEAs seem to be aware of those statistical indicators on AML regimes which the UK has endorsed in the FATF through its 40 recommendations? Why do organisations seem to infrequently join forces (e.g. couldn't the FSA and NCIS work together more often on improving the quality of SARs and feedback to industry, if not much more?)?

[70] Certain of the recommendations in this chapter have been made in the past by various sources (e.g. Gold and Levi, 1994; Dickin, 2000; Hicks, 2003; KPMG, 2003; TI, 2003; HMIC, 2004).

Why is it the case that lines of communication between LEAs and NCIS do not appear open and effective? Assigning the regime one leader, one owner, could overcome many of these problems. This owner should be held *truly* accountable for all SARs-related decisions, and—critically—should also be used to hold others to account. The owner could monitor LEA usage of Elmer; analyse LEA feedback; produce an annual report and other industry-relevant materials/feedback (based on LEA-related information); coordinate the activities of relevant government departments and agencies; provide guidance and advice to LEAs; help them to get the most from SARs; and become a centre of excellence on all things SARs/AML (many of these are sub-recommendations, below). The owner would need to be subject to regular external review by an oversight board with familiarity with the regime and the UK's AML strategy. The board would itself need sufficient power to effect change, should the owner and/or the regime begin to lose steam or to head in the wrong direction. Such a board, for example, would need greater power than that of the Home Office coordinated MLRTF, and would need to be more focussed in remit than the NCIS Service Authority. The board could be given quarterly or biannual status updates (drawing from material that would ultimately end up in the publicly available annual report). And the board could be used to give approval on contentious decisions, like the June 2004 reduction of nonconsent disseminations. This is not the first time that a report on SARs has commented on the lack of an owner. It would, however, be refreshing if it were to be the last. After all, the UK is the world's fourth-largest economy, and one of the world's financial centres. The UK's AML regime cannot realistically be run in an uncoordinated fashion with all relevant government departments and agencies working in silos without any one owner running the show.[71] The most likely candidate for the ownership role is, of course, NCIS (SOCA), given its centrality within the regime. Many recommendations below refer to the owner; this should be taken to imply NCIS/SOCA. Though not explicit, buy-in to recommendations from the owner's oversight board would be essential.

119. **Recommendation 2 (critical). The first task of the regime's owner (NCIS/SOCA)—in conjunction with all of the relevant parties within the regime (e.g. ACPO/ACPOS, HMRC, Home Office, HMT, FSA, CICFA, and perhaps MLAC)—should be to publish a mission statement that sets out the aims, objectives, and principles of the SARs regime**. Such a mission statement would clarify the extent to which the SARs regime is designed to combat only the most serious and organised crime (NIM Level Three crime) or the more local NIM Level One and Two crime, or both (both being the opinion of the author). Such a mission statement would thereby remove the kind of ambiguity that contributed to the suboptimal handling of the June 2004 reduction in nonconsent disseminations. Moreover, such a mission statement would allow for clearer resource allocation decisions. Among other things, if the intent of the regime is to combat all crime (NIM Levels One, Two, and Three), then NCIS/SOCA will need to recognise in both word and deed that many aspects of the SARs regime relate to crime which is otherwise outside its remit. And considerable effort must be expended on the day-to-day running of the regime, including on data receipt and input; database maintenance;

[71] Apropos of nothing, one wonders what the regime would look like had the independent agency approach been adopted with responsibility for the regime in its entirety (along the lines of AUSTRAC: regulator, SARs provider, and intelligence analyst).

collection and processing of management information; analysis of LEA feedback. Much of this work will not relate to SARs regarding serious/organised crime.

120. **Recommendation 3 (critical). LEAs should make constant, unwavering use of the Elmer database, including the feedback mechanism**. Sadly, it would be relatively easy for Elmer to be ignored by busy LEAs (even though the information therein would assist LEA crime-fighting activities). Elmer should be employed as a matter of course in *all* (nearly all) LEA business, particularly acquisitive crime. For example, with regard to FIUs, Elmer searches should be a mandatory part of all cash seizures, confiscations, and money laundering investigations. Elmer should be used (in FIUs and particularly FIBs) proactively to tee off investigations, and reactively, as a standard cross-check for ongoing investigations. Moreover, Elmer should be interrogated to let the data speak for themselves in an intelligence-led approach (e.g. a set of core analyses, such as who are the most disclosed upon individuals, could be conducted on a regular basis, perhaps monthly/quarterly). The use of the information contained on Elmer must be mainstreamed into daily life throughout the LEA (regardless of whether responsibility for access is maintained in FIU or FIB in the case of police LEAs).

121. **Recommendation 4 (critical). In accordance with the aims of the regime—and to encourage constant and unwavering LEA use of Elmer—LEAs should be given guidance on what is expected of them in the form of nationally-agreed minimum work standards on the use of SARs generally, the use of Elmer specifically, and the provision of feedback/statistics. Performance indicators should be introduced which mirror these minimum standards. Minimum standards should be assembled by the owner of the regime (NCIS/SOCA) in conjunction with ACPO/ACPOS, HMRC, the Home Office, ARA (given its training responsibilities), and perhaps SDEA, DWP, and NCS**. LEAs themselves made a call for such guidance. This is critical. Pre-rollout, LEAs examine those SARs which they receive through the dissemination process, as well as those sent by NCIS through search requests. With the rollout, however, LEAs will have access to the system in its (near) entirety. What, then, should LEAs do with SARs? How should SARs be prioritised for action? Should LEAs evaluate *all* SARs which appear relevant to their area on a daily/weekly basis? In so doing—and in the absence of automated checks—what cross-checks should they conduct as a matter of course, if any (e.g. PNC, local force intelligence databases, JARD, Elmer itself, etc.) to evaluate the information/develop the intelligence? Should they only work up SARs with hits on other systems? Or perhaps LEAs should only interrogate the database with specific queries, leaving the information evaluation to NCIS/SOCA and its keyword searching on national priorities (until Elmer Phase II and its advanced analytical capabilities)? Should LEAs be downloading all relevant SARs and transferring them to force intelligence databases? If so, how should this information be sanitised? What protocols should be adopted regarding the critical confidentiality of SARs? What statistics should LEAs be keeping and how? How and when should feedback be submitted (with Elmer, it will be very easy to rapidly examine a number of SARs; should feedback be submitted on each examination of a SAR, or only when a SAR is really *used*?)? The point here is not to strip the creative element from the use of SARs, but to allow LEAs to comply with any minimum standards, bringing the performance of all LEAs up to a certain minimum level (with carrots and

sticks to prevent under-performance). This minimum level should make the use of Elmer matter of course on all LEA business.[72]

122. **Recommendation 5 (critical). To encourage take-up of minimum work standards (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should monitor LEA access to Elmer and maintain management information on account logins, database searches, and SAR downloads. This information should be reported to LEA managers, as well as ACPO/ACPOS, HMRC, and the Home Office**. This information could then be used as an accountability mechanism for LEAs—comparing LEA usage to agreed minimum standards—encouraging greater use of the database. Moreover, such information could be used to illustrate levels of usage of SARs for industry and policy-makers. This appears to be the current plan, so as a recommendation this may be redundant—but NCIS/SOCA should be sure to follow through.

123. **Recommendation 6 (critical). For similar accountability purposes (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should make systematic use of the feedback provided by LEAs on their use of SARs. This information should be reported to LEA managers, as well as ACPO, ACPOS, HMRC, and the Home Office**. Feedback on SARs is of vital importance to the regime—ultimately to industry and policy-makers—and it is unfortunate that it has hitherto been largely under-utilised. NCIS/SOCA should conduct regular (e.g. quarterly) analyses of the feedback provided by LEAs. The regular analysis of feedback would provide another accountability mechanism on LEA use of SARs, and it would allow for greater understanding of the uses to which SARs are put—or why SARs are infrequently used, if this turns out to be the case. Information on typologies and trends in reporting should be sent to industry and FSA to improve the quality of disclosures.

124. **Recommendation 7 (critical). Because of associated efficiency gains for users of SARs, NCIS/SOCA should ensure that Phase II of the Elmer rollout—with its advanced analytical capabilities—is delivered on schedule**. Phase I of the Elmer rollout is most certainly a critical and exciting development in the regime. It does not deliver full functionality, however, as it represents more of a database filtering mechanism (still one that is remotely available, the critical aspect). Phase II will bring the advanced tools which will allow LEAs to more effectively and efficiently tap into the true crime-fighting potential of SARs. Phase II may ease LEA resource demands. For example, until database cross-checks are automated, LEAs must rely on manual procedures to evaluate information. The bulk downloading of SARs, part of Phase II, will greatly facilitate bulk searching of national and local databases. Otherwise, LEAs will need to download SARs one-by-one from Elmer or key-in the information to local systems by hand.

[72] Some work in this direction took place in 2000 (see Dickin, 2000). It is unclear whether or not this work was fully taken on board as national LEA policy (it does not seem to have been adopted by ACPO/NCIS). In any case, current use of such minimum standards seems spotty at best, and so much has changed in the intervening years that an updated approach is required.

125. **Recommendation 8 (critical). Because of associated efficiency gains for users of SARs, database cross-checks between Elmer and relevant national databases (e.g. PNC, JARD) should be automated, such that database hits are highlighted when looking at a SAR or series of SARs on Elmer; this should be handled by NCIS/SOCA, perhaps in conjunction with the Police Information Technology Organisation (PITO)**. Database hits allow LEAs to prioritise SARs for further intelligence development and investigation. And such prioritisation will be critical to the best use of limited resources, as Elmer will allow LEAs to see so many more SARs potentially of relevance to them than at any time in the past. The automation of database cross-checking should bring massive efficiency gains to LEAs (though not without up-front costs). Though presumably subject to some MOUs, databases for automated cross-checking would include PNC, JARD, Centaur, and perhaps others. And the idea would be to use the same IT approach to link Elmer on a local basis with local systems (e.g. force intelligence systems). This would likely require LEAs to use standardised IT solutions for intelligence databases (this is consistent with recommendations made by the Bichard Inquiry (Bichard, 2004) for a national IT system for police intelligence in England and Wales). Links between SARs themselves should also be automatically flagged up (e.g. between subject names and/or account numbers).

126. **Recommendation 9 (critical). LEAs, particularly those with the most limited SARs-related capacity, should devote greater staffing resources to units with responsibility for SARs; resources should be ring-fenced if possible**. Save for those few LEAs for whom SARs allocations may be truly limited—allocations are probably the best barometer of what is in store for LEAs with the rollout of Elmer and access to virtually all SARs—each LEA should maintain at least one specific SARs person, (far) more in the larger LEAs. Funding shortfalls could/should be addressed by the Home Office, perhaps through underspends in the Recovered Assets Incentivisation Fund. Posts should be increased not least because there appear to have been very few changes in staffing since 2002, if not before—despite considerable increases in the number of SARs filed by industry. Staff could be financial investigators, financial intelligence officers, and/or analysts/researchers/clerks. It should be accepted *ex ante* that new staff may need time to learn the ropes (there seems to be a dearth of fully trained, unemployed financial investigators/intelligence officers in the UK, so new staff will be green). Of course, all SARs-related staff nationwide will be green to some extent, as few will have played with the remote Elmer. New ring-fenced SARs staff should allow for the maximisation of SARs and the Elmer database. Such staff should also facilitate any record-keeping requirements set forth in the minimum work standards.

127. **Recommendation 10 (highly desirable). JARD should be modified to capture information on whether or not SARs initiated or otherwise played a role in cash seizures and confiscations**. Tick boxes could be added to the system, for example, to capture such information for each cash seizure/confiscation record. The statistical information obtained would assist policy-makers and industry in gauging the efficacy of the regime, at least on the asset recovery front. There would also be some overlap with information captured in Elmer feedback—but this could be used to validate data. There are limitations on the nature of questions which may be contained in JARD—responses must be factual, not subjective, so questions may be limited to something like: *one or more SARs were received on the target*. While some subjectivity would be preferable, this information will be of great importance regardless. [NB: As at mid-June 2005, the JARD

team has indicated that such changes will be include the subsequent version of JARD, currently in development.]

128. **Recommendation 11 (highly desirable). ACPO should decide who exactly within police LEAs will have access to Elmer: FIUs, FIBs, or both—and how**. The current ACPO proposal that Elmer should be given to FIBs seems incomplete. Does this imply that FIBs will have exclusive access, and that FIUs will need to go to FIBs for information—or will they have Elmer access of their own? If FIBs and FIUs both have access, a memorandum of understanding must be drafted to explicitly set forth the work requirements of each, lest scarce resources be wasted on duplicated work. The proposal should probably be designed with the full input of the ACPO working groups on intelligence, financial investigation, and proceeds of crime issues; NCIS/SOCA; and perhaps the Home Office.

129. **Recommendation 12 (highly desirable). The regime's owner (NCIS/SOCA) should publish an annual report on the SARs regime (drawing on the use of SARs by LEAs) and make it freely available via the internet**. As noted, this research is motivated in part by regulated sector calls for information/feedback on the use made by LEAs/NCIS of SARs. Such information would be most efficiently broadcast in a unified document. Indeed, this is consistent with the desires of the regulated sector. The report should be designed with industry guidance and oversight. Content of the report should be driven in large part by recommendations made by industry, and it should present any management information to be maintained by NCIS/SOCA on LEA use of Elmer, information based on the future systematic analysis of LEA feedback, and the like. Perhaps the first such report could be released in the summer of 2006, following the completion of FY 2005-06 and the launch of SOCA.

130. **Recommendation 13 (highly desirable). The regime's owner (NCIS/SOCA) and its LEA partners should ensure that lines of communication on SARs-related issues are open and functioning effectively**. There is little doubt that a certain level of mutual distrust persists between, for example, NCIS and LEAs. NCIS works hard to assemble worthwhile intelligence products, but then LEAs don't seem to know of their existence (because of complications in intelligence dissemination by NCIS, because LEA managers do not disseminate intelligence products on to staff, or because of LEA disdain for such products). LEAs discuss shortcomings in the SARs system amongst themselves, but no potential solutions ever seem to get offered up to managers at NCIS. Stronger NCIS/LEA liaison efforts could and should be made to improve regime-specific communication (e.g. intelligence product distribution methods should be reconsidered if products aren't making their way to the intended readership).

131. **Recommendation 14 (desirable). ACPO/ACPOS and the Home Office should strongly encourage LEAs to employ case management systems which allow LEA personnel to follow the progression of a case from the intelligence development stage to final outcomes—unless effective systems are already in use—to facilitate Elmer feedback and deeper analysis of SARs**. Once LEAs have a firm grasp on the sort of information expected of them (as set forth in the minimum work standards, above), they will still need to have some vehicle for capturing outcomes. Case management systems could provide such a vehicle (and Elmer is *not* a case management system). And case management systems would allow for deeper analysis of SARs than currently prevails, especially for those LEAs whose approach to SARs entails hard-copies stuffed in filing

cabinets. The units dealing with SARs who do not use any case management systems at present should either adopt systems in use elsewhere in their LEA, or the LEA in its entirety could adopt a case management system. There are costs associated with such a decision, of course: staff will need training, and it is important that buy-in to any such system is LEA-wide. This is not to suggest that LEAs should request bespoke systems, as off-the-shelf solutions may suffice (perhaps with minor modifications to allow for the recording of information pertaining to the use of SARs). There would, of course, be benefits to LEA-wide case management systems (above and beyond in facilitating the collection of data on SARs): they should allow for moderate to considerable efficiency gains LEA-wide (interestingly, many LEAs in this study called for the introduction of a uniform nationwide case management platform).

132. **Recommendation 15 (desirable). An in-depth follow-up study on LEA use and management of SARs similar to the present research should be conducted in 2006 or 2007. This is relevant especially with the rollout of Elmer, which will fundamentally change the interface between LEAs and SARs**. A number of issues face the SARs regime at present, and many of these will hopefully be ironed out in due course. It remains to be seen how improvements in the regime (particularly LEA aspects of the regime) will have an impact on crime reduction and various intermediate measures. Of course, sufficient time should be allowed for Elmer and SOCA to bed down and for any recommended actions to have been taken.

133. Recommendations are summarised in Table 15.

Table 15. Recommendations

1 (critical). For accountability purposes and to coordinate the activities of the various relevant government departments and agencies, the SARs regime should once and for all be assigned an "owner" (most likely NCIS/SOCA with a slightly expanded remit), and this owner should be governed by an oversight board.
2 (critical). The first task of the regime's owner (NCIS/SOCA)—in conjunction with all of the relevant parties within the regime (e.g. ACPO/ACPOS, HMRC, Home Office, HMT, FSA, CICFA, and perhaps MLAC)—should be to publish a mission statement that sets out the aims, objectives, and principles of the SARs regime.
3 (critical). LEAs should make constant, unwavering use of the Elmer database, including the feedback mechanism.
4 (critical). In accordance with the aims of the regime—and to encourage constant and unwavering LEA use of Elmer—LEAs should be given guidance on what is expected of them in the form of nationally-agreed minimum work standards on the use of SARs generally, the use of Elmer specifically, and the provision of feedback/statistics. Performance indicators should be introduced which mirror these minimum standards. Minimum standards should be assembled by the owner of the regime (NCIS/SOCA) in conjunction with ACPO/ACPOS, HMRC, the Home Office, and perhaps SDEA, DWP, and NCS.
5 (critical). To encourage take-up of minimum work standards (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should monitor LEA access to Elmer and maintain management information on account logins, database searches, and SAR downloads. This information should be reported to LEA managers, as well as ACPO/ACPOS, HMRC, and the Home Office

Table 15. Recommendations (continued)

6 (critical). For similar accountability purposes (as well as for feedback to industry/policy-makers), the regime's owner (NCIS/SOCA) should make systematic use of the feedback provided by LEAs on their use of SARs. This information should be reported to LEA managers, as well as ACPO, ACPOS, HMRC, and the Home Office.

7 (critical). Because of associated efficiency gains for users of SARs, NCIS/SOCA should ensure that Phase II of the Elmer rollout—with its advanced analytical capabilities—is delivered on schedule.

8 (critical). Because of associated efficiency gains for users of SARs, database cross-checks between Elmer and relevant national databases (e.g. PNC, JARD) should be automated, such that database hits are highlighted when looking at a SAR or series of SARs on Elmer; this should be handled by NCIS/SOCA, perhaps in conjunction with the Police Information Technology Organisation (PITO).

9 (critical). LEAs, particularly those with the most limited SARs-related capacity, should devote greater staffing resources to units with responsibility for SARs; resources should be ring-fenced if possible.

10 (highly desirable). JARD should be modified to capture information on whether or not SARs initiated or otherwise played a role in cash seizures and confiscations.

11 (highly desirable). ACPO should decide who exactly within police LEAs will have access to Elmer: FIUs, FIBs, or both—and how.

12 (highly desirable). The regime's owner (NCIS/SOCA) should publish an annual report on the SARs regime (drawing on the use of SARs by LEAs) and make it freely available via the internet.

13 (highly desirable). The regime's owner (NCIS/SOCA) and its LEA partners should ensure that lines of communication on SARs-related issues are open and functioning effectively.

14 (desirable). ACPO/ACPOS and the Home Office should strongly encourage LEAs to employ case management systems which allow LEA personnel to follow the progression of a case from the intelligence development stage to final outcomes—unless effective systems are already in use—to facilitate Elmer feedback and deeper analysis of SARs.

15 (desirable). An in-depth follow-up study on LEA use and management of SARs similar to the present research should be conducted in 2006 or 2007 to track progress on use of SARs. This is relevant especially with the rollout of Elmer, which will fundamentally change the interface between LEAs and SARs.

VI. CONCLUSION

134. Despite calls for more information/feedback from industry, and despite the attention brought to the regime by KPMG and others, very little was known about the LEA use and management of SARs in the UK. This report has attempted to fill the gap in existing knowledge, highlighting the often complex issues surrounding the LEA side of the UK's AML regime. It has flagged up the fact that SARs appear to be under-utilised by most LEAs; systematic information maintained by LEAs on their use of SARs is limited and often of poor quality; the information which is, in fact, maintained is under-utilised by NCIS and subsequently by the larger policy community; communication and feedback between and within LEAs, NCIS, ACPO, government, and industry is suboptimal; and positive change is afoot in the regime—especially with the rollout of the Elmer database. The report has made 15 recommendations for action which should be considered by organisations and agencies including the LEAs themselves, ACPO, NCIS, the Home Office, CICFA, and the Treasury. These recommendations should combat deficiencies in LEA aspects of the regime.

135. The SARs regime should be a powerful tool in the deterrence, disruption, and enforcement of money laundering and predicate offences. It would be a shame not to see the regime live up to its potential. It is hoped that this report will have at least some positive impact on the future processes and outcomes of the regime, particularly those aspects relating to LEAs. Time will tell.

REFERENCES

Association of Chief Police Officers of England, Wales, and Northern Ireland. "Blueprint for Policing in the 21st Century." London: ACPO, 2001.

Aldridge, Roger. "Management of SARs in Police Forces." ACPO, 2004 (internal mimeo).

Assets Recovery Agency. *Proceeds of Crime Update* and *Money Laundering News*. London: ARA, various issues, 2003-2005.

Australian Transaction Reports and Analysis Centre. *AUSTRAC Annual Report 2003-04*. Sydney: AUSTRAC, 2004.

———. *AUSTRAC Annual Report 2002-03*. Sydney: AUSTRAC, 2003.

Bentley Jenison. "SFI Audit." Bentley Jenison, 2005 (internal mimeo).

Business Executives for National Security. *Recommendations for Improving the Suspicious Activity Report*. Washington, DC: BENS, 2003.

Bichard, Sir Michael. *The Bichard Inquiry Report*. London: The Stationery Office, 2004.

Central Intelligence Agency. *Factbook on Intelligence*. Washington, DC: CIA, 2002.

Christopher, Steve. "A Practitioner's Perspective of UK Strategic Intelligence." In Ratcliffe, Jerry H., ed. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press, 2004.

Criminal Intelligence Training Coordination Strategy Working Group. *Minimum Criminal Intelligence Training Standards for US Law Enforcement and Other Criminal Justice Agencies*. Washington, DC: Global Justice Information Sharing Initiative, 2004.

Cuéllar, Mariano-Florentino. "The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance." *Stanford Public Law and Legal Theory Working Paper Series* 47 (2003).

Dickin, C. *Report on the Proposed Management Policy for Financial Disclosures*. Bristol: Avon & Somerset Constabulary, 2000 (internal mimeo).

Egmont Group. *FIUs in Action*. Egmont Group, 2000 (mimeo).

Financial Action Task Force. *Nine Special Recommendations on Terrorist Financing*. Paris: FATF, 2005 (revised).

———. *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations*. Paris: FATF, 2004.

———. *The Forty Recommendations*. Paris: FATF, 2003 (revised).

———. *Providing Feedback to Financial Institutions: Best Practice Guidelines*. Paris: FATF, 1998.

Financial Crimes Enforcement Network. *Annual Report: Fiscal Year 2004*. Washington, DC: FinCEN, 2005a.

———. *Strategic Plan FY 2006-2008*. Washington, DC: FinCEN, 2005b.

———. *The SAR Activity Review: Tips, Trends, and Issues*. Washington, DC: FinCEN/BSAAG, various issues, 2000-2005.

———. *The SAR Activity Review: By the Numbers*. Washington, DC: FinCEN/BSAAG, 2004a.

———. "FinCENnews: FinCEN Awards BSA Direct Contract to EDS." Washington, DC: FinCEN, 2004b.

———. *Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative*. Washington, DC: FinCEN, 2003.

———. *FinCEN Follows the Money: A Local Approach for Identifying and Tracing Criminal Proceeds*. Washington, DC: FinCEN, 1999.

Financial Transactions and Reports Analysis Centre of Canada. *FINTRAC Annual Report 2004*. Ottawa: FINTRAC, 2004.

———. *FINTRAC Annual Report 2003*. Ottawa: FINTRAC, 2003.

Flood, Brian. "Strategic Aspects of the UK National Intelligence Model." In Ratcliffe, Jerry H., ed. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press, 2004.

Gold, Michael, and Michael Levi. *Money Laundering in the UK: An Appraisal of Suspicion-Based Reporting*. London: The Police Foundation, 1994.

Her Majesty's Inspectorate of Constabulary. *Payback Time: Joint Review of Asset Recovery Since the Proceeds of Crime Act 2002*. London: HMIC, HMCPSI, HMMCSI, 2004.

———. *A Need to Know: HMIC Thematic Inspection of Special Branch and Ports Policing*. London: HMIC, 2003.

———. *Policing with Intelligence: Criminal Intelligence—A Thematic Inspection on Good Practice*. HMIC, 1997.

Her Majesty's Treasury. *Anti-Money Laundering Strategy*. London: HMT, 2004.

———. *Full Regulatory Impact Assessment: Money Laundering Regulations 2003*. London: HMT, 2003.

———. *Combating the Financing of Terrorism*. London: HMT, 2002.

Hicks, Tristram. *Operation Kinloss: Final Report 2003*. London: Metropolitan Police Service, 2003 (internal mimeo).

Higgins, Oliver. "Rising to the Collection Challenge." In Ratcliffe, Jerry H., ed. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press, 2004.

Hollywood, John, Diane Snyder, Kenneth McKay, and John Boon. *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior*. Santa Monica, CA: RAND Corporation, 2004.

Inland Revenue. *AML Strategy*. London: Inland Revenue, 2004 (mimeo).

International Monetary Fund. *United Kingdom: Financial System Stability Assessment including Reports on the Observance of Standards and Codes on the following topics: Banking Supervision, Insurance Supervision, Securities Regulation, Payment Systems, Monetary and Financial Transparency, Securities Settlement Systems, and Anti-Money Laundering and Countering Terrorist Financing*. Washington, DC: IMF, 2003.

International Monetary Fund and World Bank. *Financial Intelligence Units: An Overview*. Washington, DC: IMF/WB, 2004a.

———. *Twelve-Month Pilot Program of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Assessments: Joint Report on the Review of the Pilot Program*. Washington, DC: IMF/WB, 2004b.

Joint Money Laundering Steering Group. *Revised Guidance Notes (Proposed Text)*. London: JMLSG, 2005.

KPMG. *Money Laundering: Review of the Reporting System*. London: KPMG LLP, 2003.

Law Society. "News from the Law Society: New Money Laundering Guidance (22 March 2005)." London: Law Society, 2005 (online mimeo).

Levi, Michael. "Money Laundering and Its Regulation." *Annals of the American Academy of Political and Social Science* 582 (2002): 181-94.

———. "Money Laundering: Risks and Countermeasures." In Graycar, A., and P. Grabosky, eds. *Money Laundering in the 21st Century: Risks and Countermeasures*. Canberra: Australian Institute of Criminology, 1996.

———. "Incriminating Disclosures: An Evaluation of Money Laundering Regulation in England and Wales." *European Journal of Crime, Criminal Law and Criminal Justice* 2 (1995): 202-217.

Money Laundering Regulations 2003. 2003, c. x.

Money Laundering Reporting Task Force. *Second Report to Ministers*. London: Home Office/MLRTF, 2004a (internal mimeo).

———. *Report to Ministers*. London: Home Office/MLRTF, 2004b (internal mimeo).

National Criminal Intelligence Service. *Service Plan 2005/2006*. London: NCIS, 2005.

———. *NCIS Financial Intelligence Business Area (SFI): Performance Overview, July-December 2004*. London: NCIS, 2005 (internal mimeo).

———. *NCIS Financial Intelligence Report: June 2004*. London: NCIS, 2004 (internal mimeo).

———. *The National Intelligence Model*. London: NCIS, 2000.

———. *NCIS FID: Money Talks—The Strategy*. London: NCIS, no date (internal mimeo).

Office of the Auditor General of Canada. *Report of the Auditor General to the House of Commons—Chapter 2: Implementation of the National Initiative to Combat Money Laundering*. Ottawa: Office of the Auditor General of Canada, 2004.

Performance and Innovation Unit, Cabinet Office. *Recovering the Proceeds of Crime*. London: Cabinet Office, 2000.

Proceeds of Crime Act 2002 and Explanatory Notes. 2002, c. 29.

Ratcliffe, Jerry H., ed. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press, 2004.

———. "The Structure of Strategic Thinking." In Ratcliffe, Jerry H., ed. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press, 2004.

Reuter, Peter, and Edwin M. Truman. *Chasing Dirty Money: The Fight Against Money Laundering*. Washington, DC: Institute for International Economics, 2004.

Schum, David A. *Evidence and Inference for the Intelligence Analyst*. Lanham, MD: University Press of America, Inc., 1987.

Thony, Jean-François. "Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units." *European Journal of Crime, Criminal Law and Criminal Justice* (1996): 257-282.

Transparency International (UK). *Clean Money, Dirty Money: Corruption and Money Laundering in the UK*. London: TI (UK), 2003.

van Duyne, Petrus C., and Hervy de Miranda. "The Emperor's Clothes of Disclosure: Hot Money and Suspect Disclosures." *Crime, Law & Social Change* 31 (1999): 245–271.

Warner, Michael. "Wanted: A Definition of Intelligence." *Studies in Intelligence* 46 (2002).

APPENDIX I: SARS CASE EXAMPLES PROVIDED BY LEAS

LEAs were asked to provide sanitised case examples of the use of SARs. Eighteen publicly usable examples were received from 16 LEAs. It should be noted that while these case examples can illustrate the manner in which SARs do appear to contribute to crime reduction, there is little empirical merit in presenting individual case examples as sound evidence of the overall efficacy of the regime; one success-story from each LEA does not necessarily imply a well-functioning AML system. Case examples are, however, useful in indicating the range of LEA activity related to SARs, and also in suggesting to reporting entities that their efforts are not in vain (potentially motivating industry to continue to cooperate with the reporting requirements).

Despite guidance to the contrary, many LEAs provided only limited information. Time constraints prevented follow-up action to gather more detail (though there is a fine line between providing interesting detail and exposing sensitive information). Further, it is indeed disappointing that more than half of the primary LEA users of SARs provided no publicly usable case examples (33 of the 49 responding to the survey, 11 of whom provided no examples whatsoever). It is unclear if this is indicative of 1) historical lack of success with SARs; 2) limited promise of SARs; 3) limited law enforcement use of SARs; 4) no means of gathering such information; and/or 5) due to the very real possibility that the fact that one/many SARs contributed positively to a criminal justice outcome has not been disclosed in court (i.e. is not public knowledge). This last possibility is critical: industry very reasonably supports the confidentiality of SARs; such confidentiality, however, often prevents case examples from making it to the public domain.

To be fair, case examples have been in high demand recently with documents such as the HMIC 2004 *Payback Time* report; perhaps there are not sufficient examples to go around. A number of LEAs noted that interesting examples were available but not for public use—as cases/investigations are ongoing. Thirty-nine such examples were received from 25 LEAs in the course of the research, many resulting from consent SARs. Such examples should be enlightening in the future (and the information available about them indicates some novel/exciting uses of SARs), but alas they add little to the present report. There were also examples of excellent uses made of SARs in cases which ultimately fell apart in court; they are not included here.

Publicly available case examples are presented below:

- The receipt of a SAR by an LEA acted as a catalyst in the investigation of a complex financial scheme exceeding £100 million.

- A SAR was received which suggested that a money service business in the UK was transferring substantial amounts of money overseas. An investigation commenced, revealing the existence of previous SARs, one of which suggested a connection to European drug-related crime and money laundering. The business was run by two individuals, one in the UK and one in the Middle East. The individual in the UK collected money through clandestine meetings throughout the country. The individual was arrested with more than £175,000 in cash, and a further £200,000+ was recovered in various premises. The individual admitted transferring £25 million out of the country in a period of 18 months, and was imprisoned. Nearly £600,000 were

confiscated. The other individual was arrested in Europe several years later and extradited to the UK, ultimately pleading guilty to laundering £25 million.

- A SAR received from a reporting entity noted that Mr A was regularly banking large amounts of cash in the form of one pound coins, these were in round amounts and there was no form of salary paid into the account. Enquiries were commenced, and it was established that the cash was being paid into the account by the son of the account holder. Financial enquires also revealed that the father was retired and was not using the account, while the son was unemployed and in receipt of benefit. The information contained within the SAR then tied in with information held by the LEA suggesting that the son was committing offences of theft from gaming machines. A total of four men were arrested in connection with the offences and were convicted of conspiracy. Guilty pleas were submitted, and all were given terms of imprisonment. It was shown that the accused had benefited some £200,000 from their crimes, and assets were traced to the value of £82,000.

- A reporting entity made a disclosure to NCIS after Mr B instructed the entity to purchase property. The subject was at the time under investigation for drug offences. Mr B was then further investigated for money laundering, and number of accounts were discovered (of use during the confiscation).

- A SAR was filed on a drug trafficker paying cash into a third-party account under the guise of a limited company (but actually destined for a drug supplier elsewhere in the UK)—resulting in a confiscation order of some £90,000.

- Two SARs were received by an LEA indicating that a local postal official was suspected of criminality. An investigation commenced to gather evidence of criminality, which took about two years, before the arrest and charge of the official for the theft of over £750,000 from a post office. The official was sentenced to 5 years imprisonment and a confiscation order was made in the sum of over £750,000.

- The development of an intelligence package based on SARs resulted in the arrest and charge of individuals in connection with the distribution of pornographic videos.

- A number of SARs were received by an LEA relating to a number of individuals involved in exchanging large amounts of cash with travel agents. Enquiries were conducted, and all individuals were convicted of money laundering and subject to the confiscation process.

- Over a period of time, a number of SARs were disclosed by a reporting entity. These were collated by an LEA, and an intelligence package was put together for action by an operational drugs team. Family members were charged with conspiracy to supply Class A drugs. One member of the family attempted to dissipate/launder funds when released on bail. The LEA received a further SAR from a reporting entity which resulted in the family member being arrested and charged with money laundering. As a result of the SAR, the funds were secured. All family members received substantial prison sentences, and a £170,000 confiscation order was made.

- In 2003, a reporting entity requested consent regarding a transaction involving more than €1.3 million. Consent was granted, and the money was seized. Despite

contending the seizure on human rights grounds, the defendant did not supply a statement nor did he appear in court. In 2004, the court ruled in favour of the LEA, forfeiting the funds.

- SARs led to the investigation of a large UK business (with turnover of billions of GBP). Through NCIS, an LEA was provided with a volume of information that detailed the ownership and nature of transactions going through offshore companies. The UK companies would buy materials from connected tax haven companies and the UK group was reporting large losses. The offshore arrangements were never static, however, and during the course of enquiries the LEA became aware of over 40 offshore companies. There were myriad issues including company residence, transfer pricing, branch/agency, trust legislation and employee remuneration arrangements. Ultimately the case settled for more than £6 million.

- A two-year investigation of a major drug trafficking operation was conducted, and nine individuals were arrested. Financial investigations were undertaken alongside the criminal investigation, and substantial assets were identified both in the UK and SE Asia, held in the name of various family members of the 'top man'. Two SARs from two different reporting entities, received over 12 months apart, located additional accounts that would otherwise not have been identified, resulting in more than £100k being added to the assets available for confiscation. A confiscation order of more than £3 million was ultimately made.

- In 2004, a consent SAR was received by NCIS from a reporting entity seeking consent to move funds in divorce proceedings (there were questions surrounding the source of funds). Consent was refused to move £200,000 on behalf of the husband. After an investigation, the husband was arrested and convicted of a £2 million fraud.

- In 2003, an LEA received a SAR from a reporting entity relating to a large deposit of cash. An operation was mounted and the LEA arrested a European national at Waterloo Station on suspicion of money laundering. The individual was just about to board a Eurostar train to France and was carrying a large bag containing more than £150,000, which were seized. A detailed money laundering investigation was launched, involving enquiries in the United States, Europe, and an offshore jurisdiction, though no prosecution was ultimately taken forward. However, the evidence gathered during the course of the investigation showed clear links to unlawful conduct. No legitimate claim was ever made on the money, and the funds were successfully secured through a forfeiture order.

- As a result of a SAR-based intelligence package developed by an LEA, enquiries were undertaken into the affairs of two individuals working for the UK subsidiary of a multinational manufacturing firm. Mr E ordered fictitious goods and services on behalf of the company and subsequently authorised that the goods had been received and passed on sales invoices from a fictitious supplier for payment. The firm paid all such invoices into the account of this supplier, believing it to be a company account—whereas in fact it was the personal account of Mr E's ex-wife, Ms F. The majority of the funds were then forwarded on to Mr E. Both individuals were arrested for conspiracy to defraud.

- A woman was dealing heroin from her home address and duly convicted. Whilst the confiscation investigation was in progress, a reporting entity read in the local paper about the conviction. A SAR was submitted, and assets were restrained.

- Mr G, who had originally entered the UK in 1997 as an agricultural worker (and who had been denied asylum but remained in the UK illegally), set up an employment agency supplying workers to the agricultural industry with the help of a co-defendant. The agency traded from 2000-2003, employing up to 250 workers, all of whom were illegal immigrants and all of whom were supplied with forged Home Office documentation by the agency. The agency supplied up to 35 other companies with labourers. Income into the company was assessed as more than £4 million; £3 million was withdrawn in cash to pay to workers and owners. SARs from reporting entities who were alerted by the size of cash withdrawals led to the investigation of the agency. Six people were ultimately arrested, receiving custodial sentences ranging from three to seven years. A confiscation order was made against all six for £1.7 million.

- A reporting entity disclosed suspicious activity on an account. Enquiries revealed that the account was controlled by another person, Mr H. Mr H was arrested, and a search revealed him to have 100+ identities and to be systematically defrauding various banks (all with stolen identities). Mr H and an accomplice received custodial sentences. Mr H was also ordered to pay more than £250,000 following a compensation hearing.

APPENDIX II: EXAMPLES OF GOOD PRACTICE IN SARS MANAGEMENT (PROCESSES)

Certain good practices in SARs management were uncovered in the course of the research, though numbers of good practices worthy of discussion and replication in other LEAs were not overwhelming. The rollout of Elmer represents such a fundamental change the interface between LEAs and SARs that separate Elmer-related good practices should be released by NCIS in due course, particularly on getting the most out of the system (e.g. novel/effective/efficient uses of the data-mining and filtering technologies of the system). This will become all the more relevant with Phase II of the rollout in 2006.

Three good practices are briefly described below:

Information management: Inland Revenue and the Metropolitan Police Service. One of the drivers of the present report is a lack of feedback from LEAs/NCIS to industry. While a rolled out Elmer will allow for much greater use of SARs and will provide an online feedback facility, Elmer is not a case management system. LEAs will need to have an understanding of how SARs were used in their units; this is the information which can then be fed back to NCIS. In the event, both Inland Revenue and the Metropolitan Police Service have developed IT solutions in-house. Both are based on commercially-available software (IR using MS Access; MPS using Cardbox software). The systems are simple and perhaps not overly elegant, but—and this is the key—they are functional. Critically, both allow for an understanding of the use made of SARs in the units (though once intelligence packages leave the units, neither solution can track the ultimate outcomes of packages; this needs to be addressed separately), and both allow for case management. Both also allow for much deeper searching and analysis, though the MPS solution seems more suited for this. Elmer's analytical tools, notably with Phase II of the rollout, may obviate the need for powerful analytical capabilities in these IT applications. Admittedly, the applications seem to some extent focussed on tracking SARs upon receipt, as opposed to the outcomes of deeper information interrogation. This could presumably be changed.

Evaluation/development/investigation decisions: Scottish Drug Enforcement Agency. One of the recommendations of this research relates to a set of minimum work requirements for LEAs on SARs, including the manner in which SARs are evaluated upon receipt. While the goal is in no way to remove creative decision-making on SARs development, a number of LEAs appear to follow a standard decision-making flow chart approach which sets forth 1) what is done as a matter of course with SARs upon receipt; and 2) how such SARs are prioritised for further investigation. A good example of this is the SDEA, which employs a flow-chart approach to the evaluation of SARs upon receipt; the flow chart guides decision-making on whether or not SARs should be subject to further intelligence development (and ultimately investigation, though investigations will be carried out by other units; the flow chart also generally specifies who is responsible for what). All SARs will be subject to certain database cross-checks. If certain criteria are met (e.g. hits on one or more databases), the SAR or SARs may be assigned for further development. (Admirably, the SDEA's approach takes advantage of Scotland's bulk-searchable intelligence databases (e.g. the Scottish Intelligence Database, SID). This allows for efficiency gains in the minimum work process.) This is not to suggest that all SARs should undergo complex evaluation upon receipt; maximising the benefit of SARs likely requires as much if not more work centred on interrogating the information (see the NCIS good practice example below) as development upon receipt. The point here is that because *some* evaluation of SARs upon receipt will need to be carried out (perhaps

electronically, with some form of advanced keyword searching/automated database cross-checking), the most efficient approach appears to be that guided by an easily understood formal decision-making model.

Interrogating the information: National Criminal Intelligence Service. As noted in Chapter III of the present report, SARs may be evaluated upon receipt (and subsequently developed/investigated if appropriate); SARs may also be subjected to deeper interrogation/analysis of the *who are the most prolific offenders* sort. LEAs themselves appear to be doing little in the way of the deeper interrogation/analysis (though this will hopefully change with the rollout of Elmer, particularly Phase II). A current example of good practice in information interrogation is that of NCIS in its work on identifying the most-disclosed-upon individuals. This work recognises explicitly that SARs may often be received relating to the same individual—but from sufficiently different postcodes that territorial LEAs will not pick up on them when looking at only SARs relating to their responsible geographical area. Without getting into the detail (as this is a public document), it would seem that this type of analysis and others like it represent an excellent use of SARs. LEAs should carry out such information interrogation on a regular basis. In fact, it is not difficult to imagine that several analytical approaches could be assembled and run monthly or quarterly for both tactical and strategic purposes; these could even be built into the web-enabled Elmer. NCIS obviously does this type of work with national targets—and LEAs would not want to simply duplicate work being done elsewhere—but various information interrogation analyses could be based more on local and regional information/intelligence, and these could be run by LEAs.

[Blank page]