Appendix 7.4: Data-mining system and FIU capacity to filter fast in detail[[1]](#footnote-1)

In **Austria**, reports are sent by email, fax, post and courier. All reports are manually integrated into the FIU database. The Austrian FIU is a law enforcement unit and this means that it has to systematically start criminal proceedings for each piece of information received from a reporting entity which meets the requirements of an STR in order to clarify the suspicion of a criminal act. It is relatively hard to compare receiving and analysing STRs in Austria, as an investigation is started for almost all STRs received.[[2]](#footnote-2) The FIU has no own analytical tool in the sense of data mining. Moreover, the Austrian representatives did not consider data-mining tools very helpful.

In practice, the **Belgian** FIU receives 70% of STRs electronically and 30% in writing. The electronic system through which reports are submitted to the FIU is a system that FIU Belgium has developed itself. The Belgian FIU has introduced since 2006 a system of online reporting. Institutions or professionals that want to report electronically can ask the FIU for a login code and password. The electronic reporting system contains a certain format that the reporting entities must fill in. The STRs that are received in writing mostly come from the non-financial sector. Finally, the entire analytical process is done manually, meaning that there is no preliminary ‘red flag’ or automatic system that filters out STRs that are not further analysed. Hence, there is no automatic pre-analysis available to the Belgian FIU.

In **Bulgaria,** the STRs can be forwarded by the reporting entities online,[[3]](#footnote-3) but according to the FIU representatives, this is currently done manually – by post.[[4]](#footnote-4) The reporting entities must make use of a standard reporting form, which has been approved by the director of the FIU. The analysis of reports is done for one part manually and for another electronically, but given the increase in the reports received from the obliged entities the FIU is planning to invest further in an IT support platform for their analysis. According to the FIU representative, the Bulgarian FIU already uses several visualization software and document management systems, and its own system has certain data-mining properties.

According to the **Cypriot** representative, the FIU receives the SARs by post, or manually. However, the FIU has just finished organizing a digital reporting system which they have already connected to the servers of the three largest banks in Cyprus. They plan to expand this to all other banks. For data mining, MOKAS uses a I2 IT system. The system was reported to be user friendly and helpful in revealing red flags among suspicious patterns of financial transactions and in allowing the investigators to visualize the flows of money and thereby to easily identify the more complicated ML financial constructions.

In the **Czech Republic**, the FIU analysts use the I2 analytical software, the ELO document management system and MoneyWeb as well as their own analytical system. This helps the analysts ‘assess the information requested for the analysis, to trace the movement of funds and to determine the profile of the persons (both natural and legal) involved in the STR’.[[5]](#footnote-5) According to the Czech representative, these IT systems accommodate almost all STRs, especially since 90% of the STRs are electronically submitted. The remaining 10% of STRs reach the FIU via a letter or fax. These are submitted in general by smaller practices and entities that do not often report.

The **Danish** FIU usually receives reports by fax. According to the Danish representative, Denmark is in the process of a change, because GoAML should have started working at the end of August 2011. It was then expected that the majority of reports would be disclosed electronically. Moreover, with GoAML there will be an initial automatic analysis, which makes a pre-selection of interesting cases. Only then will inspectors proceed to analysis and subsequent criminal investigation. It is unclear whether online/electronic reporting has been put in place in the meantime. The website of the FIU does not allow for online reporting.

In **Estonia**, since January 2008 the reporting entities have been able to send a notification to the FIU electronically by using the digital format on the website of the FIU. According to the Estonian representative, the RABIT IT system the FIU has in place allows the automatic analysis of the STRs, but does not perform an automatic analysis. The staff of the FIU will therefore analyse all reports. If there is no further suspicion, the STRs are archived.[[6]](#footnote-6)

**Finland’s** FIU database was created as part of the criminal intelligence database of the Finnish Police. This in turn was problematic because it was not created to support the analysis of STRs and these had to be registered and analysed manually.[[7]](#footnote-7) According to the Finnish representative, the situation has changed. Reports are currently mostly handed in electronically, by email and in April 2011 the Finnish FIU was using the GoAML system.

The incoming **French** STRs are analysed by the members of the analysis department of TRACFIN with the help of a complex and powerful data-mining system – STARTRAC. Reporting entities can report electronically, by mail or by fax. Since June 2012 TRACFIN has opened a telecommunications service ERMES statement. This remote procedure should facilitate the reporting of professionals subject to the FIU. Nevertheless, the FIU representatives mentioned that information is not lost if transmitted by mail/post. Due to the geographical size of France, the latter simply takes longer, which is why TRACFIN encourages the usage of electronic reporting.

In **Germany**, the FIU reports that approximately 99% of STRs are submitted electronically or by fax. STRs that are received in hard copy are digitized and also captured as electronic documents in the FIU database.[[8]](#footnote-8) Furthermore, according to FATF (2010e), when a new STR is entered (by the FIU or the Land police unit) into the STR database, there exists an automatic data-mining system that cross-checks the information against other STRs in the database and against all police databases to which the introducing agency has access.[[9]](#footnote-9)

In **Greece,** an STR from a bank is sent to the AML/CTF/SFI Authority. The Chairman of the Authority decides which of the three subordinate units receives the report. This is not mutually exclusive and the ML/TF cases are forwarded to the FIU. Until recently the receiving of STRs was done manually and at present 60% of the credit institutions report electronically, according to the Greek representatives. The FIU offers the possibility of reporting online through a secured connection.

In **Hungary**, the FIU appears to be adequately funded and provided with sufficient technical and other resources to fully and effectively perform its functions. The AML/CTF Act requires obliged entities to report electronically and this has prompted some discussion as to whether not allowing any paper reporting would not create disincentives for DNFBPs. The Hungarian authorities have argued this would not be the case and that electronic tools were tailor-made for the needs of the reporting institutions, and that the FIU provides technical support for any party wishing to report.[[10]](#footnote-10) Finally, MONEYVAL (2010c) reported that the HFIU has its own data-mining system (HUFO).[[11]](#footnote-11)

In **Ireland** about 70% of STRs are disclosed by means of electronic reporting. The reporting system is developed by the FIU in cooperation with the designated bodies. The smaller reporting institutions are often the ones that report manually, as the electronic system is quite expensive. The Irish FIU representative argues that one would need to do a cost-benefit analysis for the smaller reporting entities and see whether putting in place a secure system for information transmission is cost efficient. Given these reasons, the fact that 30% of reports are submitted on paper is not seen as problematic. Furthermore, the Irish representative reports that the FIU has a data-mining system in place.

In **Italy**, reporting was produced electronically and delivered by post until May 2011. In May 2011 the FIU introduced a new system – called RADAR – for reporting STRs in order to improve the quality and timeliness of reports. The new reporting system introduces a standard reporting form (with clear requirements to detail the description of the transaction as well as the reasons for suspicion) and the possibility of reporting electronically.[[12]](#footnote-12)

According to the **Latvian** representative, the FIU receives reports very differently. There has been an increase in the number of reports sent electronically. Since 2010 twenty of the largest reporters in Latvia have only been reporting electronically. Small practices, however, still report on paper. With respect to the analysis, according to the Latvian representative, the FIU database is not linked to other databases. This implies that scanning of reports is done manually by an FIU employee and not automatically, as in Estonia. However, the Latvian IT system provides for additional alerts when an individual involved in the STR is put on the EU watch list.

The **Lithuanian** reporting system is not fully computerized and this was reported to have created problems in terms of the deadlines set for the reporting institutions.[[13]](#footnote-13) According to the Lithuanian representative, dealers in precious stones do not report electronically. Nevertheless, banks report electronically using an online matrix in addition to submitting a written report. This is a considerable improvement as the reports from the banks constitute 95% of the FIU’s work. With respect to the analysis of the information received, the FIU has an IT system and analytical software that are both up to the challenge.[[14]](#footnote-14)

All STRs are analysed by the FIU **Luxembourg**. It receives reports by any means – electronically, by fax and by mail or by personal delivery. The banks which file the most STRs use USB sticks to forward this information to the FIU. The FIU is considering putting in place a more rapid electronic reporting system. The FIU has no data-mining system for its database. Financial information is analysed with tools like Excel and this is done by a financial analyst. The authorities are considering implementing a data-mining system. In summary, the authorities are considering creating an electronic system for receiving STRs, putting in place a data-mining system and rewriting the IT database system of the FIU.

In **Malta**, the reporting is not yet digital. According to the Maltese representative, the FIU prefers receiving reports in person. This way they are sure STRs do not get lost and that nothing impedes them from reaching the FIU. With respect to the IT system, the Maltese representatives tell us that the FIU has developed its own IT software. The FIU has looked into getting more sophisticated software, but this is very costly. It has therefore applied twice to the EU to obtain funds to buy GoAML,[[15]](#footnote-15) but this has been denied twice. It therefore plans to acquire the I2 analytical software to enable it to perform network analyses faster.

FIU-NL is currently implementing a new computerized system (GoAML) that will contain both unusual and suspicious transactions. This system offers many new possibilities for data examination and analysis. However, due to the slightly different internal nature of the FIU – the mix of administrative staff and police using two databases (UTRs and STRs) – it needs further adjustments.[[16]](#footnote-16) For more than a year, all reports have to be sent electronically to the FIU. Furthermore, the FIU has put in place a web application enabling reporting entities to safely report. This is fast and secure, according to the FIU representative. The **Dutch** FIU receives the vast majority of UTRs in an electronic format. UTRs can be filed directly with the FIU with protected software that all reporting institutions can use, after registering on the website of the FIU.[[17]](#footnote-17) In addition to the UTRs received from the reporting entities, the FIU also receives information that may be related to money laundering, in the form of requests for information, which are forwarded to the FIU by law enforcement agencies through the office of the public prosecutor.[[18]](#footnote-18) These requests are checked for relevance and the information to be provided is reclassified from UTR to STR and then disclosed to the law enforcement agencies.

The **Polish** FIU is well equipped with technical and information technology facilities. The employees carrying out the strategic analysis of the data are supported by modern IT tools that allow them to create and apply module solutions in their analysis.[[19]](#footnote-19) Furthermore, the FIU seems to make use of its own data-mining system – although this is not explicitly mentioned in its annual reports.

The **Portuguese** FIU receives STRs from the obliged entities electronically. They have their own IT system. The FIU also allows for reporting using their website as a platform.

In **Romania,** most STRs are sent electronically, but according to the Romanian representative, the FIU cannot refuse notifications it receives on paper, hence the receipt system can never be fully electronic. The FIU pays a great deal of attention to the IT system supporting the data analysis. The FIU is endowed with an ‘own IT system’.

The **Slovak** FIU is responsible for receiving UTRs and it can do so electronically or manually. According to the FIU representative, reports are still mostly received manually. Plans to improve the IT support of the FIU have been approved and will be introduced shortly. In this sense new communication software (MoneyWeb) will be introduced to ensure faster and more reliable communication between the FIU and the obliged entities.[[20]](#footnote-20)

In **Slovenia** reports are sent to the FIU either electronically or in hard copy. According to the Slovenian representative, the FIU does not receive too many STRs, because it has trained the banks to report only very suspicious transactions (to prevent over-reporting). The FIU receives about 200 STRs per year and it can open an investigation into each of them. The OPML does not seem to have an automatic data-mining system, but the latter still needs to be confirmed by the country representatives.

In **Spain**, all STRs (whether suspicious or systematic reports) coming from notaries and financial entities are sent digitally to SEPBLAC. SEPBLAC has developed software for this, and basically all institutions send their communications to SEPBLAC this way – in fact they are obliged to do so by law.[[21]](#footnote-21) STRs from DNFBPs are still submitted manually (on paper), but this does not constitute a large fraction of the total inflow of reports. With respect to further analysis, SEPBLAC has developed its own database and digital system, together with some private companies.

According to the **Swedish** representative, all covered entities need to register as a reporting entity with the FIU in advance. Initially, the FIU received different forms of STRs both electronically and in a paper format, but since 2010 STRs have only been submitted electronically. The FIU has introduced technical tools and databases for improved analysis of information – i.e. iBase and Analyst Notebook – which allow for an initial digital screening and cross-checking of STRs.[[22]](#footnote-22)

According to the **UK** FIU representative, 98% of SARs are received electronically. Progress continues to be made on reducing the number of SARs submitted on paper (by fax or post) and the UK FIU continues to encourage electronic submission. The UK FIU makes all but the restricted SARs available to UK LEA to read and investigate via the extranet portal MoneyWeb. SARs relating to consent, integrity, terrorism, counter-proliferation, finance and PEPs are proactively analysed and disseminated by the UK FIU. In their analysis, the UK FIU makes use of various data-mining analytical tools.[[23]](#footnote-23)

1. This is an online appendix to *The Economic and Legal Effectiveness of the European Union’s Anti-Money Laundering Policy,* Chapter 7. [↑](#footnote-ref-1)
2. FATF (2009c), p. 73. [↑](#footnote-ref-2)
3. Available at: http://www.dans.bg/en/msip-091209-menu-en/reporting-11a-31012011-mitem-en.html. [↑](#footnote-ref-3)
4. Available at: http://www.dans.bg/images/stories/FID/guidelines\_reporting\_lmml\_lmft-02082012.pdf. [↑](#footnote-ref-4)
5. FATF (2011), ‘Fourth Mutual Evaluation Report on the Czech Republic’, p. 68. [↑](#footnote-ref-5)
6. MONEYVAL (2008b), p. 71. [↑](#footnote-ref-6)
7. FATF (2007b), p. 66. [↑](#footnote-ref-7)
8. FATF (2010e), p. 102. [↑](#footnote-ref-8)
9. FATF (2010e),p. 100. [↑](#footnote-ref-9)
10. MONEYVAL (2010c), p. 53. [↑](#footnote-ref-10)
11. MONEYVAL (2010c), p. 74. [↑](#footnote-ref-11)
12. FIU Italy (2010), ‘Annual Report’, p. 6. [↑](#footnote-ref-12)
13. MONEYVAL (2010), ‘Second Third Round Progress Report on Lithuania’, p. 90. [↑](#footnote-ref-13)
14. Ibid., p. 68. [↑](#footnote-ref-14)
15. GoAML available at: http://goaml.unodc.org/. [↑](#footnote-ref-15)
16. From email correspondence held with the representatives on 07.05.2012. [↑](#footnote-ref-16)
17. FATF (2011b)*,* pp. 97–8. [↑](#footnote-ref-17)
18. Ibid., p. 98. [↑](#footnote-ref-18)
19. MONEYVAL (2007a), p. 56. [↑](#footnote-ref-19)
20. MONEYVAL (2011b), p. 66. [↑](#footnote-ref-20)
21. Articles 18(3) and 20(2) of the 10/2010 law and Article 13 of the Royal Decree 925/95. [↑](#footnote-ref-21)
22. FATF (2010c), p. 32. [↑](#footnote-ref-22)
23. SOCA UK FIU (2011), ‘SARs Annual Report’, pp. 9–11 and 14. [↑](#footnote-ref-23)