Identity Protection or not for Employees Reporting Money Laundering? The UK Case

Simonova, Anna

Publication date:
2011

Document version
Early version, also known as pre-print

Citation for published version (APA):
Simonova, A. (2011). Identity Protection or not for Employees Reporting Money Laundering? The UK Case.

IDENTITY PROTECTION OR NOT FOR EMPLOYEES REPORTING MONEY LAUNDERING? THE UK CASE

ANNA SIMONOVA [*]

The article highlights an issue which has received renewed attention due to the UK case Shah v. HSBC Private Bank determined by the Court of Appeal. The issue is the extent of identity protection of employees who are legally required to report suspicion of money laundering to the authorities. In its recent judgement, the court opens up for the possibility of disclosure of identities of reporting employees to a customer, thereby challenging the assumption that such employees are subject to public interest identity protection.

I INTRODUCTION

All financial institutions are required to comply with anti-money laundering (AML) measures. One of them is reporting suspicion of money laundering. This requirement means the following. If suspicion is reported to authorities and consent is granted by the authorities to proceed with the transaction in question, then the financial institution is not at risk of being prosecuted. Suspicion is defined as a possibility which is more than fanciful that the relevant facts exist. A vague feeling of unease does not suffice.[1]

Even though suspicion is inherently subjective, the UK legislation is very clear about sanctioning failure to report suspicion where there are reasonable grounds for suspecting money laundering.[2] The Joint Money Laundering Steering Group (JMLSG) Guidance states that the test of reasonable suspicion is objective. The test would likely be met when there are demonstrated to be facts or circumstances, known to the member of staff, from which a reasonable person engaged in a business subject to the Money Laundering Regulations would have inferred knowledge, or formed the suspicion, that another person was engaged in money laundering.[3]

---

[*] *PhD fellow, the Law Faculty, the University of Copenhagen, Studiestraede 6, 1455, Copenhagen, Denmark. anna.simonova@jur.ku.dk*

1 Blair W & Brent R(2008) Banks and Financial Crime: The International Law of Tainted Money, Oxford University Press, p.167

2 Proceeds of Crime Act 2002, sections 330 & 331

3 The JMLSG Guidance, Part I, par. 6.15

Financial institutions generally owe a duty of confidentiality towards their customer. The duty means that financial institutions have no right to disclose customer information to third parties unless such disclosure is authorised in exceptional circumstances. Disclosing suspicion of money laundering is an exception to the general rule. Financial institutions and their employees will not incur liability for disclosing customer information if such disclosure is made in the course of compliance with AML reporting obligations.[4]

II SHAH V HSBC PRIVATE BANK

The recent case Shah v. HSBC Private Bank highlights another related issue - the issue as to whether identities of employees involved in the reporting process can be disclosed to a customer. The case is about two customers who sued their bank for delays in effecting their payment instructions on four occasions.[5] The delays were up to 2 weeks. No evidence of money laundering was found by the police. It was alleged by the claimants that the delays had caused them economic loss and compensation was thus claimed. The delays resulted from the bank's disclosure of suspicion to the authorities and anticipation of the authorities' consent to proceed with the transactions. The claimants challenged that the bank employees had really held that suspicion. The bank refused to disclose the identities of the employees involved in the reporting process except for the identity of the Money Laundering Reporting Officer.

Financial institutions naturally have an interest in protecting their employees due to the risk of harm. There is no British statute which specifically and explicitly grants employees of financial institutions public interest immunity in the AML context. There are only recommendations in favour of that. These recommendations come from public bodies such as the British Bankers Association, the Home Office and the Serious Organised Crime Agency which is authorised to receive suspicious activity reports (SARs).[6] Information on identities of all employees involved in the reporting process is not asked for in the SAR form. Normally the form only asks for the identity of the nominated officer or any other contact person appointed to disclose SARs to the authorities.

As it has been held by the Court of Appeal in the recent case, customers may require financial institutions to prove the held suspicion in a non-summary trial proceeding.[7] The question of good faith/bad faith is relevant for the proof of the

---

4 Proceeds of Crime Act 2002, sections 337 & 338

5 Shah & anr v HSBC Private Bank (UK) Ltd (2009) Case No. IHQ/08/0530IHQ/08/0786

6 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2011) Case No HQ07X03152, par. 44

7 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2010) Case No: A3/2009/0461, par. 39

held suspicion.[8] This means that financial institutions will potentially be required to disclose how, when and from whom these suspicions emanated. Lack of knowledge about the precise identity of the individuals involved in the reporting process may be considered to be a litigious disadvantage suffered by the claimant.[9]

The Court of Appeal opened up for a possibility of disclosure of more details surrounding the reporting process.[10] Having weighed up the public interest in confidentiality and the public interest in open justice, the Court ordered the bank to identify the departments the involved individuals had worked for and give each of them a letter.[11] This order provided the claimant with an opportunity to get an idea as to the spread of employees involved in the reporting process on four occasions.

If it became apparent that one or two individuals was repeatedly and closely involved in the writing or receipt of relevant reports on all four occasions, then the claimants would be able to seek the detailed identity of any such employee. If the spread of employees involved turned out to be wide, then it would be more difficult to obtain the detailed identities of such employees.[12]

The Court made this order in the light of three circumstances. Firstly, the claimants were not, and were not at the time, involved in money laundering according to the police investigation. Secondly, the bank's employees were not at any risk of reprisals or physical harm from the claimants. Thirdly, the reality of the situation was such that the claimants already had a good idea of the identity at least some of the individuals involved.[13] The timing of disclosure of information about the involved employees does matter as the Court of Appeal made it clear.[14] While such disclosure remained doubtful during the time when investigations into the customers' financial affairs were still under way, that disclosure could take place at a later stage.

III CONCLUSION

Confidentiality of identities of reporting employees is thus not absolute even though the courts will be approaching an eventual disclosure in a gradual and cautious manner. The onus is on financial institutions to prove the held suspicion. They will potentially be required to show the basis on which the suspicion was formed, by

---

8 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2011) Case No HQ07X03152, par. 10

9 Ibid, par.26

10 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2010) Case No: A3/2009/0461, par. 39

11 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2011) Case No HQ07X03152, par. 51

12 Ibid, par.52

13 Ibid, par.46

14 Jayesh Shah, Shaleetha Mahabeer v HSBC Private Bank (UK) Limited (2010) Case No: A3/2009/0461, par.39

whom, when and how. Given the burden of proof, the reporting process needs to be designed carefully. The reporting process has to prevent situations, where one individual employee acts out of bad faith, and ensure the wider spread of employees involved in the reporting process. In large financial institutions, it is easier to accomplish due to a large staff turnover. Meanwhile, this task becomes more challenging in smaller financial institutions.

The reporting regime has to be made more flexible. In other EU countries there is no consent requirement.[15] This means that it is a legal defence for financial institutions to report suspicion of money laundering without awaiting consent to proceed with the suspicious transaction in question. As the above case shows, authorities' long processing time does no good for a customer relationship. In fact, the long processing time creates additional legal risks for financial institutions by exposing them to the risk of being sued in contract and tort. Secondly, in other EU countries the reporting regime is more flexible in connection with postponed reporting. For example, financial institutions may postpone reporting suspicion if the transaction in question cannot be delayed or if reporting suspicion may alert the customer or otherwise prejudice an investigation.[16] The example of situations where the transaction cannot be delayed is when the customer risks violating his contractual obligations due to transaction delays.[17] In the UK, financial institutions may postpone reporting if there is a reasonable excuse to do so.[18] In the Treasury approved guidance, only one example is given in this connection. When a transaction which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the nominated officer may need to let the transaction proceed and report it later. Meanwhile, the guidance makes a reservation by saying that the reasonable excuse defence is untested by case law and would need to be considered on a case-by-case basis.[19]

The practice of other countries shows that there is more than one approach to the reporting regime. The current fight against financial crime depends on the public-private partnership. The value of suspicious activity reports supplied by financial institutions has been acknowledged by law enforcement authorities. Against this background, it is of importance to ensure that the public-private partnership does not create additional legal risks for financial institutions. Granting reporting employees statutory identity protection and eliminating or modifying the consent requirement are two possible reforms of the current reporting regime.

---

15 Denmark is an example of such EU country lacking the consent requirement.

16 Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme nr 389 af 15/04/2011/The Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism nr 389 of 15/04/2011, § 7 (3)

17 The Danish FSA's Guidance to the Act on Measures to Prevent Money Laundering and Financing of Terrorism, par. 50

18 *Proceeds of Crime Act* 2002, section 330 (6a) & 331 (6)

19 The JMLSG Guidance, Part I, par. 6.47