The European fight against terrorism financing: Professional fields and new governing practices

Wesseling, M.

Citation for published version (APA):
Chapter 6.

Theatre of Compliance: the Third AML/CFT Directive in Practice

There is no evidence that the Third Directive is essential or cost-effective in the fight against terrorism financing.
—Interview at the European Commission, 2009

There is a clear difference between being compliant with the Third Directive and combating terrorism financing.
—Interview a compliance officer, 2010

6.1 Introduction

The Third Directive on the prevention of the Use of the Financial System for the Purpose of Money Laundering Terrorist Financing (2005/60/EEC) (henceforth, the Third Directive) is the European Union’s most important and comprehensive instrument for fighting terrorism financing. Adopted in 2005, it requires businesses in the banking and financial services sectors to store and monitor their clients’ data and to make risk assessments to detect suspicious transactions. The Directive is a ‘preventive effort’ to combat terrorism via the financial system and has three proclaimed objectives (EU, 2005, p. 15). In Foucauldian terms these can be called ‘ideal functions’, the functions we expect the Directive to perform (Foucault, 2007, pp. 117-118, see also chapter 3).

First, the Third Directive requires regulated entities to identify their clients and to monitor their transaction data in order to detect terrorists and their associates. Due diligence procedures, meaning the detailed identification of the customer and assessment of his financial behaviour, are considered of ‘crucial importance’ for the prevention of terrorism financing (EU, 2005, p. 16). Likewise, the analysis of ‘risky’ transactions, for instance those involving large cash payments, is thought able to uncover terrorist intentions and should be reported.

A second objective of the Directive is to disrupt terrorist plots by denying terrorists access to their funding and thereby cutting off their ‘lifeblood’. This means that banks should refuse any service to entities blacklisted as terrorism suspects. Similarly, they have to report
suspicious transactions pertaining to terrorism financing to the national Financial Intelligence Unit (FIU) and, if requested by the FIU, furnish all necessary information (ibid., p. 27).

Third, according to the Directive, the transfer of legally or illegally obtained money for terrorist purposes through the financial system can jeopardize the stability and the reputation of, and confidence in, the financial system. The Directive intends to protect ‘the soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole’ by establishing European norms integrating international FATF recommendations (EU, 2005, p. 15).

So far, the Third Directive has been studied primarily by legal scholars, and by a few political scientists and economists. A significant portion of this work consists of detailed assessments of the content of the law and analyses of the Directive in relation to the broader legal context. Mitsilegas and Gilmore (2007), for instance, examined the evolution of the EU’s three AML Directives and addressed the challenges they pose to the EU’s legislative and constitutional framework. They raised questions with regard to the legitimacy of EU action in this field – does the EC/EU have the legal competence to adopt global standards – and the compatibility of the Directive with the protection of civil liberties and certain fundamental rights, in particular the confidentiality of the lawyer-client relationship. Taking a more descriptive approach, Handoll (2006) devoted a chapter to the Third Directive. He offered a detailed legal analysis, discussing the legal basis, objectives, structure, key definitions, requirements and obligations of the Directive. A comparative analysis between the legal requirements of the FATF and those of the EU’s anti-money laundering framework has been undertaken by Van den Broek (2011b). She highlighted that despite the fact that the Third Directive aims to transpose FATF recommendations, there is a certain amount of discrepancy between the norms as defined by the EU and those of the FATF.

A few other academic works have focussed on implementation of the Third Directive. Bergström et al. (2011) studied the Third Directive as an example in which for-profit actors are given a role in assuring national security, and how this new role could jeopardize democratic accountability. They concentrated especially on differences in implementation of the Directive between the UK and Sweden. An early-stage assessment of the implementation of the Third Directive in Italy was offered by Costa (2008). Taking only the anti-money laundering aspects of the Third Directive into account, he concluded that the Directive improves the definition of money laundering in Italian legislation as well as the organizational structure for combating money laundering.
Building on these two strands of existing academic work, this chapter offers a micro-level analysis of the daily practices and modes of governing developed to comply with the Third Directive’s objectives and examines its power implications. Although literature on the Directive is growing, the detailed workings of the regulatory framework remain more or less unknown. This chapter examines the new professional field that has emerged from the requirements of the Third Directive. It considers how public and private authorities ‘co-produce’ intelligence to fight terrorism (Favarel-Garrigues et al., 2009), and how the exercise of power is dispersed across numerous places and people. It also specifically investigates new practices of governing that have been established in response to the Directive. How are accounts monitored continuously? How are customers qualified as risky? Which transactions are considered suspicious? Furthermore, questions are raised concerning the implications of fighting terrorism financing through the private sector. What are the societal and political implications of this cooperation in the case of the Third Directive, for instance, with regard to democratic accountability and transparency?

An examination of banks’ daily practices for combating terrorism is all the more important in the light of the thin results yielded by the Directive’s requirements, as highlighted in the impact assessment reports of consultancy firms and national auditing agencies. In reports for the European Commission, consultancy firms conclude that compliance with the Directive is sufficient but that the effectiveness of the Directive is difficult to measure because of a ‘lack of quantitative and limited qualitative information’ (Deloitte, 2011, p. 293). Moreover, they argue that it is difficult to measure success because the preventive effect of the recommendations can hardly be measured at all (John Howell, 2007, p. 26). The Dutch National Audit Office states that the results of the AML/CFT legislation have been disappointing. It ‘insufficiently prevents against terrorism financing’ and, ‘the chances of terrorism financing being discovered and punished are small’ (Algemene Rekenkamer, 2008, p. 15). Similarly, during fieldwork interviews, civil servants at the European Commission stated that ‘there is no evidence that the Directive is essential or cost-effective’ (interview 10) with respect to combating terrorism financing. This finding raises the question of what precisely the purpose of the Directive is, if not efficiency in the sense of amounts of assets frozen and successfully prosecuted terrorist financiers. In this chapter I argue that although the objective of the Third Directive is to inhibit the financing of terrorism, it sets in motion an apparatus of compliance in which compliance itself has become the main objective.
In order to investigate the field of governing and the governing practices emerging from the implementation of the Third Directive in detail, I shall use the metaphor of a ‘theatre of compliance’. In this chapter, the theatre is the field of governing emerging from the implementation of the Third Directive. It is ‘the autonomous microcosm set within the social macrocosm’ (Bourdieu, 2000). The main objective of the field has become compliance with AML/CFT legislation. The advantages of examining the field of governing through the theatre metaphor are threefold and relate to the terminology of the theatre, the understanding of the theatre as a productive space, and the theatrical effects of the implementation of the Directive.

The terminology of the theatre is helpful because it facilitates a detailed analysis of the way in which the professional field works. Sketching the stage of the theatre helps to explain in which settings the ‘play’ (i.e. compliance) takes place and how the play is organised. The image of the stage helps to describe the (geographic) locations on which compliance is enforced and which departments within the bank are involved. It allows for assessing which actors (the participants in the field) are relevant for implementation of the Third Directive, and for describing their role. Analysing the script of the theatre play helps us to understand the governing practices through which compliance is organised. This entails a meticulous description of how AML/CFT policies create measurements on the basis of risk modelling, how scenarios operate and how transactions are deemed suspicious. Finally, the performance can be understood as the staging and representation of the results generated by the implementation of the Third Directive. Analysis of the performance also raises the question of who the audience is in this theatre.

The theatre metaphor can also be used to illustrate ‘the production of a space in which “appearance” of a particular kind becomes possible’ (Nield, 2006, p. 64). This reference to the theatre emphasizes that compliance with the Third Directive is not only a technical issue but also a social activity created by human beings. Although the legal text of the Directive might seem clear cut, the implementation appears to be far from self-evident, and can be downright messy. In fact, the Third Directive does not exactly prescribe how banks must comply, but imposes a risk-based approach. This means that in order to be compliant, banks produce their own risk categories, CFT policies and procedures against which they assess the risks posed by customers and their transactions. In turn, these procedures call into being certain performances (behaviours) by customers.

Considering the Third Directive as a productive space by looking at the professional field and its governing practices is a way of investigating the Directive from a
governmentality perspective. Examining the implementation of the Directive in terms of the stage, the script and the performance of the theatre of compliance is ‘to be sensitive to the complex geographies of power beyond pre-established scales’ (Larner & Walters, 2004, p. 14). This metaphor allows a consideration of practices of governing that affect all banking clients, and it emphasizes the dispersion of power and responsibility across an infinite number of actors in the theatre.

Finally, the discrepancy between the intended and actual results can be called the theatrical effect of the implementation of the Third Directive. As one bank employee states, ‘there is a clear difference between compliance with AML/CFT legislation and combating terrorism financing’ (interview 14).

As described in chapter 3, international measures to fight terrorism financing have often been grafted on to pre-existing anti-money-laundering frameworks. This is also true for the European Union, where the CFT dimension has been added to existing AML legislation and resulted in the Third AML/CFT Directive. To provide more context to on how the ‘theatre of compliance’ came into being during the 1990s and the first years of the new millennium, it is necessary first to give a short description of the legal scope and the political decisions upon which the Third Directive is built. Next, the choice of the theatre metaphor for analysing the governance practices of the fight against terrorism (financing) is discussed. The subsequent sections examine the stage, the scripts and scenarios and the performance of the theatre of compliance that are set in motion through the Third Directive.

6.2 The Development of the EU’s Anti-Money-Laundering Directives

6.2.1 The First Anti-Money Laundering Directive

In the 1980s, the US War on Drugs galvanized international concern regarding profits from drug trade. European states and the European Community actively supported the development and adoption of international measures aimed at combating money laundering (Gilmore, 2004, Mitislegas & Gilmore, 2007). In these years, the European Parliament demanded Community action with respect to the illegal drug trade. The financial aspects of the drug trade and money-laundering practices were first mentioned in an EP Resolution, and in the European Council Conclusions of 1986. Subsequently, the European Commission became involved in negotiating the 1988 United Nations Convention against the Illicit Traffic
in Narcotic Drugs and Psychotropic Substances, and the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. These two conventions defined, for instance, what money laundering is, and sought to criminalise money laundering through international law. Parallel to these initiatives, international standards and coordination aimed at preventing money laundering were enhanced by the establishment of a Financial Action Task Force and the adoption of its 40 Recommendations in 1989.

In 1990, the European Community undertook formal discussions regarding the adoption of European anti-money laundering legislation. This resulted in a Council Directive on the Prevention of Use of the Financial System for the Purpose of Money Laundering (91/308/EEC), (henceforth, the First Directive). The justification for a European initiative in addition to pre-existing international ones followed a ‘two-fold threat rationale’, combining a threat to the financial system and financial institutions and a threat to society in terms of health, life and the social fabric (Mitsilegas, 2003, p. 55). Other justifications for adopting the Directive were the need to protect the European Single Market from criminal money, and demonstrating to the outside world (in particular to the US) that the EC was acting in a united manner and going beyond existing international legislation by adopting preventive and legally binding instruments (Bergström, 2011, pp. 105-106, Gilmore, 2004, pp. 194-195, Mitsilegas, 2003, pp. 55-56). In addition, adoption of the Directive was also presented as ‘one of the most effective means of opposing this form of criminal activity’ (European Communities, 1991).

The final text of the Directive was adopted in 1991 and brought money laundering under Community law. It adopts not only the criminalization approach of the UN and the Council of Europe instruments prohibiting and penalizing money laundering, but also a preventive approach based on the 40 FATF recommendations in the form of imposing duties on credit and financial institutions in order to stop money laundering. The adoption of the Directive is remarkable for two reasons. It indirectly gives the European Community competence in the sphere of criminal law, which it formally does not have (Bergström, 2011, p. 105, Mitsilegas, 2003, p. 58), and it extends the fight against money laundering to the private sector, recognizing that ‘the financial system can play a highly effective role’ (European Communities, 1991).

More specifically, the First Directive required credit and financial institutions to establish customers’ identity and keep records of their transactions, the ‘Know Your Customer’ or KYC principle. Moreover, credit and financial institutions are obliged to actively report any suspicious transaction to the authorities responsible for combating money laundering, and have a passive duty to provide all necessary information at the request of
these authorities. A corollary of the duty to report suspicious transactions is the obligation to demonstrate due diligence in monitoring transactions. Hence, credit and financial institutions have to examine whether any transaction is likely to be related to money laundering, in particular complex, unusual, large transactions or sequences of transactions following strange patterns, or those involving countries that comply insufficiently with the FATF recommendations. Furthermore, credit and financial institutions have the duty to refrain from transactions of which they suspect any relation with money laundering until they have further instructions from the authorities combating money laundering. The obligation of nondisclosure to the customers concerned and third persons the information transmitted to the authorities (no tipping off) is another duty provided for in the Directive.

The first decade following the adoption of the First Directive must be seen as a ‘pioneer phase’ in which practices and procedures for the transfer of suspicious transaction data from the private sector to competent authorities and the follow-up on this information were shaped (Vedder & van Nunen, 2003, p. 72). During the 1990s, banks did not consider reporting suspicious transactions a priority, and their AML policies remained rather limited (interview 15). The main responsibility for crime prevention rested with public actors, and the dichotomy between the public and the private sector was not challenged by private actors (Bergström et al., 2011, p. 1049). It also took some time to organize the information-receiving side. There was no agreement on an internationally accepted model for the functions of a FIU (Financial Intelligence Unit) in the early 1990s (IMF, 2004, p. 9), since each country preferred a model best fitting its own objectives and institutional architecture. Moreover, within states, various agencies competed over the responsibilities emerging from the Directive, attempting to strengthen their own position in the field (see for instance Vedder & van Nunen, 2003).

The First Directive is nevertheless important because it introduced a preventive approach to money laundering in which the private sector has to report suspicious transactions to competent national authorities, later qualified as Financial Intelligence Units. This rationale and reporting structure has been maintained, extended and enhanced, in subsequent AML Directives (see table 6.1).
Successive inclusion and extension of reporting entities

| First AML Directive (1991) | - Credit institutions as defined in Directive 77/780/EEC  
- Financial institutions carrying out operations as defined in Directive 79/267/EEC  
- Insurance companies |
| --- | --- |
| Second AML Directive (2001) | Extension of the definition of financial institutions to include investment firms and collective investment undertakings  
Inclusion of:  
- auditors, external accountants and tax advisors  
- real estate agents  
- some operations of notaries and independent legal professionals  
- dealers in high value goods such as precious stones or metals or works of art  
- casinos |
| Third AML/CFT Directive (2005) | Extension of the definition of dealers in high-value goods to natural or legal persons trading in goods worth € 15,000 or more and paid cash.  
Inclusion of: Trust or company service providers |

Table 6.1 Successive inclusion and extension of reporting entities.

6.2.2 The Second Anti-Money Laundering Directive

Throughout the 1990s, a number of arguments were raised to revise the First Directive. Firstly, the European Council emphasized the link between money laundering and organised crime (see for instance European Council, 1999). Although the text of the First Directive related not only to drug trafficking offences but also to the broader notion of criminal activity, there was a perceived need to explicitly extend the predicate offences listed in the Directive. Secondly, it was argued that money launderers had circumvented AML legislation by making use of sectors outside the realm of the Directive (Mitsilegas, 2003, p. 86). Therefore, the scope of professions concerned by AML legislation needed to be widened ‘outside the classical financial sector’ (European Council, 1996). Thirdly, it was argued that not only had money launderers changed their modus operandi, but also the banking sector had changed during the 1990s. Developments in technology made some parts of the Directive outdated, and new developments, such as possibilities resulting from generalized access to the Internet had to be included (Gilmore, 2004, p. 201). A fourth aspect that needed to be addressed was the improvement of information exchanges between FIUs. The European Council stated that ‘regardless of secrecy provisions applicable to banking and other commercial activity, judicial authorities as well as FIUs must be entitled, subject to judicial
control, to receive information when such information is necessary to investigate money laundering’ (European Council, 1999). A fifth argument concerned the need to transpose new international legislation and guidelines into European legislation. These consisted most notably of the updated FATF recommendations of 1996.

Taking into account all these issues, the European Commission scheduled a proposal for a Second Anti-Money Laundering Directive in 1999. Yet, it took over two years of debate to adopt a new text. The main issues of contention were the definition of the predicate offences and the decision on the range of professions covered by the Directive (Gilmore, 2004, Mitsilegas, 2003). Following the revised FATF Recommendations, the Second Directive referred to money laundering in relation to organised crime instead of (drug-related) criminal activity. This meant that the provisions of the new Directive also applied to organised crime, fraud, corruption or any other illegal activity damaging or likely to damage the European Community’s interests (European Union, 2001). The European Parliament’s Committee of Citizens’ Rights initially preferred a more restricted definition of organised crime than the European Commission, the Council, and finally a majority in the Parliament. The Citizens’ Rights Committee also objected to the Council’s extension of predicate offences to a broad notion of serious crime (Lehne, 2000). Yet, again, in the plenary session of the Parliament, a majority was in favour of the Council’s definition.

The European Parliament’s debate on the extension of professions concerned by the Directive was even more heated. The Second Directive extended the professions with a reporting duty to currency exchange offices, money transmission remittance offices, casinos, dealers in high value goods, external accountants, auditors and tax advisors, lawyers, notaries and real estate agents (see table 6.1). The inclusion of the legal profession led to especially fierce objections by the European Parliament. Many MEPs were deeply concerned that inclusion of the legal profession would violate the right to a fair trial and the principle of lawyer-client confidentiality (Gilmore, 2004, p. 203, Wahl, 2010, p. 131). They considered that the legal profession should benefit from broader exceptions with regard to some of the requirements of the Second Directive, a point they finally obtained. On the other hand, the EP wanted to include a much wider range of professions than the Council and the Commission. The latter concluded that for practical and definitional reasons an extension to dealers in art works and luxury goods would be problematic (Mitsilegas, 2003, pp. 95-98). Finally, the ‘9/11’ attacks increased pressure on the Parliament during the conciliation procedure and provided another justification for quickly revising the existing AML legislation (Lehne, 2001, p. 7). Finally, the Second Directive was adopted on 4 December 2001.
In sum, the Second Directive brought European legislation in line with international standards and adapted it to new money laundering practices and the latest technological developments. It broadened the scope of predicate offences as well as the regulated professions. It also strengthened the customer identification requirements, especially in case of non-face-to-face operations using computers. In addition, a new provision as to the information exchange of Suspicious Transaction Reports (STRs) was added, insisting on compliance with the FATF recommendation on the establishment of an FIU in each member state.

However, due to the fact that for pragmatic reasons the notion of a “competent authority” (i.e. the FIU) was left undefined, a heterogeneous landscape arose in which broadly four different models for reporting STRs can be distinguished (see table 6.2). Quite some EU member states adopted an administrative reporting model, in which regulated professions report suspicious transactions to an administrative body, for instance the Ministry of Finance, the central bank, or an independent body. This means that an independent administrative body investigates the justification of a STR before transferring this information to law-enforcement agencies. One of the advantages of this model consists of the ‘buffer’ it creates between the financial sector and law-enforcement authorities in charge of investigating and prosecuting financial crime (IMF, 2004, pp. 10-11). Others opted for a police model in which reporting entities send their reports to a law-enforcement agency. The rationale behind this model is the possibility of employing the existing institutional framework and existing expertise of financial crime units (ibid., pp. 13-14). A few EU member states chose a judicial model, in which the FIU is situated in the office of the public prosecutor. This model can be seen as more independent from political interference and as efficient with regard to the speed of receiving suspicions and prosecuting offences (Mitsilegas, 2003, p. 169, IMF, 2004, p. 16). Two countries adopted a hybrid model that combines the characteristics of at least two models. This model ‘serves as disclosure intermediary and a link to both judicial and law-enforcement authorities’ (Masciandaro, 2007, p. 66). The distinctions between these models are important, as different rules for data exchange and protection apply to information depending on whether it is gathered in an administrative, police or judicial context. In order to facilitate information exchange between the different FIUs of the EU member states, a Council Decision was adopted in 2000 (2000/642/JHA).
Typology of FIUs in the EU

<table>
<thead>
<tr>
<th>Administrative model (11)</th>
<th>Belgium, Bulgaria, Czech Republic, France, Italy, Malta, Poland, Romania, Slovenia, Spain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police model (11)</td>
<td>Austria, Estonia, Germany, Hungary, Finland, Ireland, Lithuania, Portugal, Sweden, Slovakia, United Kingdom</td>
</tr>
<tr>
<td>Judicial model (3)</td>
<td>Cyprus, Denmark, Latvia, Luxembourg</td>
</tr>
<tr>
<td>Hybrid model (2)</td>
<td>Greece, the Netherlands</td>
</tr>
</tbody>
</table>


6.2.3 The Third Anti-Money Laundering/Combating the Financing of Terrorism Directive


However, the relatively quick adoption of the Third Directive should not be taken to mean that it consisted of only minor changes, or that it was accepted without opposition. The Directive extends the existing reporting requirements to new professions (see table 6.1) and new predicate offences. It also attempts to improve some of the shortcomings of the Second Directive, providing more guidance on customer identification requirements, for example. Moreover, it elaborates on some of the issues left undefined in earlier Directives, for instance, by describing the work and powers of FIUs and introducing the supervision of compliance and sanctions in case of non-compliance. Finally, repealing and replacing the First and the Second Directives, the Third Directive represents a qualitative shift in purpose, and consequently in the way the Directive operates as a governing practice. Two new elements are of particular importance to the Third Directive: an explicit inclusion of the fight against terrorism financing, and the embracing of a risk-based approach.

The extension of the Directive to include terrorism financing was considered a logical step in the War on Terror. It evidences the importance of anti-money laundering legislation as a central component in the global strategy to undercut terrorist financing (Mitsilegas & Gilmore, 2007, p. 125). According to the legal text ‘the preventive measures of the Directive...
should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes’ (European Union, 2005, p. 16). The definition of terrorist financing adopted in the Directive is similar to the definition expressed in the 1999 UN Convention on the Suppression of Terrorism Financing and involves:

the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (ibid., p. 20).

According to the text of the Third Directive, terrorism financing often involves international transactions, cash transactions, criminal or clean money, and may also concern service providers outside the financial sector.

Whereas the explicit inclusion of terrorist financing in the Third Directive was presented as indispensable after 11 September 2001, it is interesting to recall that during discussions of the First Directive, terrorism was excluded from the draft in the early 1990s. In the First and Second Directives, the Commission decided to adopt a minimum standard approach defining the money laundering of proceeds of ‘criminal activity’ as applying to drug offences as specified in the Vienna Convention, and other criminal activity designated as such for the purposes of this Directive by each member state (Mitsilegas, 2004, pp. 66-68). Hence, EU member states could individually decide to include terrorist offences within the scope of the Directive, but prior to 9/11 most countries did not consider this necessary.

A second major change of the Third Directive was its shift from a ‘rule-based approach’ to a ‘risk-based approach’. The rule-based approach that characterized the First and Second Directives entails the application of a set of fixed norms to every transaction. In order to assess transactions, these norms must be very detailed and clear, as, for instance, the obligation to report every cash transaction that exceeds the amount of €15,000 (Van den Broek, 2011a, p. 171). One bank employee describes it as follows:

The rule based-approach is very much a check-the-box exercise. For instance, you go down the questionnaire and if you have 27 positive responses and 3 negative ones, it means that the transaction scores 27 points. If 25 points is the established threshold, it means that the transaction is suspicious and must be reported. It also works the other way around: if a transaction is 66% normal and the norm for reporting is below 60%, then the transaction becomes considered as completely unsuspicious (interview 14).

Banks have been increasingly opposed to the rule-based approach, which they consider ineffective and requiring a disproportionate allocation of resources. The rigid character of the norms effectively meant that all transactions had to be considered in the same way without
much reflection. Moreover, it was thought that criminals who were aware of the norms were able to adapt their transactions accordingly (Unger, 2007, Van den Broek, 2011a).

Since 9/11, risk has become crucial in waging the War on Terror. Risk management is ‘a particular mode of governing – a means of making an uncertain and unknowable future amenable to intervention and management’ (Amoore & De Goede, 2008b, p. 9). Governing through risk does not imply the reduction of existing risks, but an attempt to calculate them. It is rather about upholding the ‘myth of control and manageability’ by dealing with uncertainty in an organised way (Power, 2004). Adopting the lens of risk is to look at the world from a specific perspective in which control of the financial sector can be strengthened while the mobility of money continues and becomes even easier in some cases (De Goede, 2006, Bergström, 2011).

The risk-based approach adopted in the Third Directive focuses on transactions responding to specific combinations of criteria instead of monitoring *all* transactions. It allows for differentiation between different kinds of risk such as customer risk, product or services risk, and geographical risk. As a consequence, monitoring practices and identification requirements vary according to the risk scores assigned to the profile of the customer, the specific financial product or the services and countries involved in a transaction. In the terminology of the Directive, a distinction can be made between ‘simplified due diligence’ procedures for certain customers and ‘enhanced due diligence’ procedures imposed on others. Moreover, the norms are not only differentiated according to the kind and level of risk, but they are also flexible. Risks are evaluated according to changing terrorism financing trends and profiles. The proclaimed advantage of these malleable risk criteria is that criminals cannot adapt their behaviour to avoid attracting attention to their transactions. Finally, transaction monitoring is carried out continuously. In addition to an assessment at the time the account is opened, banks are also required to monitor customer accounts and transactions on an on-going basis. As such, unusual or out of the ordinary transactions are flagged almost instantly.

The risk-based approach introduced in the Third Directive addresses some of the main shortcomings of the rule-based approach. Regulated professions obtained much more flexibility and discretion with respect to transaction monitoring procedures. It was hoped that they might thereby avoid unnecessary administrative burdens and design procedures to be more cost-effective. Moreover, the risk-based approach ‘brings great efficiency in the system (…) in that it enables banks to dedicate their resources to those things which are of higher risk and (…) those customers of lower risk cannot be burdened with undue due diligence and such alike’ (House of Lords, 2009a, p. 25). In addition, the quality of the reports was expected to
be better, because banks could direct their attention to more limited sets of transactions and file STRs on the basis of reasoned judgement, instead of a general questionnaire. ‘[Banks] have to look at clients, our products and perhaps even whole [economic] sectors’ (interview 14). This, it was believed, would result in a more effective framework for combating money laundering and terrorism financing. However, one must bear in mind that the definition of and the value assigned to a specific risk are not readily established. The quality of reports and the effectiveness of the reporting system therefore depend largely on the design of the risk management software and the expertise of compliance officers.

As a governing practice, the risk-based approach requires more active behaviour on the part of banks. Reporting entities must be able to demonstrate that they have ‘adequate and proportionate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication’ to identify and prevent the terrorist financing risks their business faces (European Union, 2005, p. 29). Consequently, the requirements of the Third Directive entail a shift of responsibility and authority from the public sector to the private sector in the field of national security (Bergström et al., 2011, De Goede, 2006, Unger, 2007, Van den Broek 2011a).

Although both the inclusion of terrorism financing and the shift to a risk-based approach were widely supported, the adoption of the Third Directive was controversial for several reasons. The main issue was the question of individual privacy rights versus security interests. The LIBE Committee of the EP concluded that the proposal for the Third Directive ‘belongs in the grey area in which individual rights and freedoms may have to be sacrificed in the higher general interest of preventing and repressing terrorist activity’ (Nassauer, 2005, p. 148). However, two MEPs, Giusto Catania from Italy and Sylvia-Yvonne Kaufmann from Germany, maintained their minority opinion opposing the text of the Third Directive and stated that ‘control and surveillance are weighed far higher than the protection of civil liberties’ in the fight against terrorism financing (Borghesio, 2005, p. 9).

Furthermore, the European Parliament considered that the compromise reached in the Second Directive regarding the reporting duties of lawyers and notaries needed clarification. MEPs doubted whether ‘the complete confidentiality of the information communicated to a lawyer is still guaranteed’ when these professionals are required to report suspicious transactions (Nassauer, 2005, p. 82). This issue was also actively taken up by different interest groups. In a letter to the European Commission, the Council of the Bars and Law Societies of Europe (CCBE) called for delaying the Third Directive. They argued that the implementation
of the Second Directive had not yet been evaluated. The CCBE also repeated their claim that this Directive ‘breaches the fundamental rights of EU citizens’ and highlighted ‘that no research into the human rights’ and civil liberties’ effects of the Second directive has been carried out’ (CCBE, 2005). In addition, French Bar associations sent a petition to the European Commission in 2003 warning that the normal activities performed by lawyers could be impeded by the requirements of the Third Directive (Petition 693/2003, see also Nassauer, 2005, p. 149). They also brought a challenge before the Conseil d’État regarding the compatibility of the Second Directive’s requirements and the right to a fair trial based on independent lawyers and confidential lawyer-client relations. Likewise, the Belgian Bar Association asked the Belgian Cour d’Arbitrage to consider the same issue (CCBE, 2006, p. 2).

Representatives of banking and financial institutions were opposed to some of the new definitions and concepts described in the Third Directive. They heavily lobbied MEPs to convince them that the disclosure requirements imposed would be far too heavy a burden on their sector and suggested many amendments (EurActiv, 2005). Of particular concern were provisions on ‘politically exposed persons’ (PEPs). The Directive defines these as ‘natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons’ (European Union 2005, p. 22). These include, for instance, heads of state or of government, senior politicians, senior government, judiciary or military officials, senior executives of state-owned corporations, and important political party officials (House of Lords, 2009b, footnote pp. 31-32). According to the text of the Third Directive, foreign PEPs and their immediate family should be subject to enhanced due diligence procedures while low risk clients, for instance public authorities or actors providing State services, qualify for simplified due diligence procedures. The decision to single out this group of people must be seen in the light of several corruption scandals of which the ‘Abacha affair’, named after the Nigerian President and members of his inner circle who stashed away over 2.2 billion dollars in foreign bank accounts, received a lot of publicity (interview 14). Banks argued that it would be very challenging to identify all PEPs worldwide. The European Banking Industry Committee also maintained that the definition of a PEP stands in contradiction with the risk-based approach in that it included everyone, not only those posing a genuine risk (Euractiv, 2005). However, these arguments were overridden, as the inclusion of PEP requirements into the Third Directive stems from international agreements, such as the FATF’s guidelines and the United Nations Convention against Corruption.
MEPs and banks also objected to the requirement to identify and verify, on a risk-sensitive basis, the ‘beneficial owner’ of the bank account. This is ‘the natural person(s) who ultimately owns or controls the customer and/or the he natural person on whose behalf a transaction or activity is being conducted’ (European Union, 2005, p. 22). Based on a FATF recommendation, this requirement aims to identify the shareholders involved in corporate transactions. However, MEPs argued that the Commission’s initial proposal to identify all shareholders possessing or controlling 10% or more of a company is ‘overly ambitious and leads to unnecessary and onerous checks’ (Nassauer, 2005, p. 115). The European Banking Industry Committee considered that the concept of beneficial owner was ‘too restrictive’ (EBIC, 2005, p. 5). Likewise, the Federation of European Banks stated that ‘banks do not have access to reliable information which would enable them to properly identify beneficial owners’ (EurActiv, 2005).

Other issues raised in relation to the Directive concerned, for instance, the implications for universities and business schools of the requirement to investigate any cash payment of over €15,000 for possible money laundering (KPMG, 2005) and the possibility for hotels providing money exchange facilities to be exempted from reporting obligations if they fulfilled certain criteria.

MEPs also questioned the lack of evidence regarding the effectiveness of the Third Directive. Already in the discussions preceding the adoption of the Second Directive, MEPs argued that ‘it has not yet been possible to prove any links between reports of suspicious transactions and convictions for money laundering or predicate offences’ (Lehne, 2000, p. 26). The main complaints in the discussions about the Third Directive consisted of the fact that the effectiveness of the Directive remained still unknown because the Directive had not yet been assessed and was in some cases not even transposed into national law (Nassauer, 2005, p. 83, 121). British Conservative MEP Theresa Villiers (EPP) stated, for instance, that there had been no serious scrutiny into the existing AML legislation, and that she had come to the conclusion that ‘these rules do almost nothing to catch criminals or terrorists and merely provide inconvenience to law-abiding citizens in carrying out innocuous everyday financial transactions’ (Villiers, 2004).

A related issue of contention, but of procedure rather than content, was the haste of the procedure. Both MEPs and professions covered by the Directive complained about the urgency of some member states and the European Commission to adopt a new AML/CFT directive. In fact, the deadline for EU member states to transpose the Second Directive into national law was June 2003, but approximately half of them had done so by that time. When
the Commission tabled the proposal for a Third Directive in 2004, the assessment of the Second Directive, required according to the text of the Directive, had not been made.

Despite this opposition, the European Parliament rejected a majority of the proposed amendments. The Third Directive was approved by the EP on 26 May 2005 and formally adopted on 26 October 2005 during the UK’s Presidency of the EU. It was recognized that further legislative measures would be needed to deal with various technical issues in order to achieve a consistent implementation across the European Union. Those measures are now contained in an Implementing Measures Directive that came into force on 24 August 2006. The Directive was to be transposed into domestic legislation before 15 December 2007. However, in mid-2008, 15 EU member states had not complied with this requirement. The Third Directive has been amended by Directive 2008/20/EC of the European Parliament and of the Council of 11 March 2008. A Fourth Money Laundering Directive is currently envisaged, and an official proposal from the Commission is expected in 2013, integrating the latest revisions of the FATF recommendations.

The three Money-Laundering Directives have strongly shaped the European institutional architecture for combating terrorist financing and money laundering, notably through the establishment of Financial Intelligence Units (FIUs) and an obligation on an important number of private actors to supply information for national security reasons. However, it must be emphasized that the Third Directive differs significantly from the earlier AML Directives by its inclusion of the fight against terrorism (financing) in addition to combating money laundering. Moreover, the Third Directive alters considerably the initial AML framework by introducing a shift from a rule-based reporting system to a risk-based approach. The analysis of Third Directive practice shows how the Directive gave rise to a new field of governing and led to new governance practices. It also draws attention to the potential uncertainty, controversy and arbitrariness embedded in the execution of the Directive. The following section provides a theoretical discussion about the use of the theatre metaphor and explains how the notion of a ‘theatre of compliance’ contributes to a detailed examination of the Third Directive from a governmentality perspective.
6.3 Theatre of Compliance

Academics have used the metaphor of the theatre in several ways to describe aspects of terrorism as well as combating terrorism. The parallels between the theatre and (counter-)terrorism’s use of mass media have been especially attractive to explore. As early as the 1970s, Brian Jenkins wrote that ‘terrorism is aimed at people watching, not at the actual victims. Terrorism is theatre’ (1974, p. 4). He stressed that to be effective, terrorists create *dramatic* and carefully *choreographed* events capturing their *audiences* and generating maximum media attention for their demands. More recently, the use of the theatre metaphor in relation to terrorism has been taken up by other scholars. Similar to Jenkins, Gabriel Weimann stresses the importance of mass media for terrorism through his notion of the ‘theatre of terror’ (1983, 2006, 2008). He states that terrorists write the *script* and perform the *drama* while media may provide the *stage* to access worldwide *audiences* (2006, p. 38). In his view, the terrorist act is a theatric performance that is given a stage by the media.

Beatrice De Graaf (2010) argues that terrorist acts create a ‘theatre of fear’. Continuing the theatre metaphor, she states that media reporting or prosecution of terrorists in court can become a *performance* and provide a *podium* for terrorists to expose their case, and for the judicial authorities asking for greater punishments. The theatrical aspects of criminal proceedings are underscored by the staging of highly protected courtrooms, the creation of new prisons, the adoption of dramatic security measures during the proceedings, or suspects’ refusal to cooperate. This was, for example, the case in the trials of members of the RAF and the Brigate Rosse. Contrary to Weimann, De Graaf argues that the success of terrorists in creating a theatre of fear depends mostly on the reaction of the population to the attack, as well as on the capacity of the state and the terrorists to influence popular perceptions (*ibid.*). In sum, the works of Jenkins, Weimann and De Graaf use the terminology of the theatre to emphasize that terrorist acts and (combating) terrorism are a strategy of expression and communication to either draw people’s attention to terrorists’ objectives or to ‘*stage* the state’ (De Graaf, 2010, p. 261, emphasis added).

This chapter also adopts the terminology of the theatre, but the theatre metaphor will have slightly different purposes. The notion of a theatre of compliance will be used to further an understanding of EU’s fight against terrorism financing through implementation of the Third Directive and to demonstrate how some aspects of the Directive are theatrised. The terminology of the theatre helps to make the professional field of governing visible as well as
its governing practices. There are also communication aspects to the implementation of the Third Directive. Banks, for instance, have an interest in complying with AML/CFT requirements because press articles about non-compliance could seriously damage a bank’s reputation. However, this chapter is not directly concerned with the influence of mass media on efforts to combat terrorism financing.

A few scholars have used the theatre metaphor with respect to daily security practices. In his essay ‘The Psychology of Security’, Bruce Schneier (2008) distinguishes between the reality of security and the feeling of security. He uses the term ‘security theatre’ to describe security measures that only increase citizens’ feelings of security and do not influence the reality of security. One such security measure is, for example, the introduction of photo ID checks in office buildings. Schneier points out that ‘no one has ever explained why verifying that someone has a photo ID provides any actual security, but it looks like security to have an uniformed guard-for-hire looking at ID cards’ (2009). Another example of security theatre is the posting of National Guard troops at American airports after 9/11. They served to decrease the anxiety of the passengers rather than prevent hijackings or bombings (Schneier, 2003, p. 38). This element of managing the impact of terrorism by reassuring the population through measures that make them feel safer is also present in the implementation of the Third Directive.

Nield (2006) addresses the theatricality of the border. She examines how border spaces reflect a particular spatial imaginary and produces the individual who attempts to cross. She argues that the contemporary border ‘is not quite there’, fixed in a specific place (p. 69). Rather, the border appears in the bureaucratic production of it, and through the staging of mechanisms of regulation governing migration. These mechanisms ‘compel certain kinds of appearance’ (p. 64) and require border-crossers to simultaneously be present (as actors) and to represent themselves effectively (as characters). In addition, Nield stresses that ‘while appearing to be stable, and the same for everyone,’ the rituals that are part of crossing the border are not neutral instruments but ‘construct and perform difference’ (p. 67). The function of the border is thus not limited to marking a territory in which certain rules apply, but also serves to construct the national imaginary, giving a sense of belonging to some and excluding others (2006, pp. 66-67). Nield’s work is interesting because she draws attention to the border as a productive space, but also as a site that constructs national imaginaries and differentiates between insiders and outsiders. Like the mechanisms of border security, the procedures and practices of the Third Directive perform the idea of a clean financial sector free from dirty
money, and they establish norms defining who can (not) be part or make use of the formal financial system.

Amoore and Hall (2010) examine the ‘border theatre’ and investigate the theatrical rituals of border security – scanning, screening and verifying identity – to which we have become used and which we have ceased to question. They ask how surprising artistic encounters with techniques and technologies of security can revive and strengthen public engagement with border practices. In their view, the border resembles a theatre in the sense that border rituals are a matter of display or show. The space of the border ‘is a political stage for the performance of control’ suggesting ‘securability and controllability’ (p. 303). Moreover, the border is also productive, like the theatre, in the sense that it permanently creates and questions appearances and identities. It brings into being series of recognizable categories, such as state authorities, illegal aliens and risky travellers, and requires border crossers to appear in a certain way by demanding specific behaviours and responses.

To start questioning the security practices at the border and to understand the assumptions on which they are based, Amoore and Hall affirm that the principles of Berthold Brecht’s epic theatre are of interest. This form of theatre uses interruptions of the sequence in order to draw attention to the existing conditions. Like the theatre, border security practices also depend on repetitions and sequences.

It is precisely these too little noticed repetitive sequences of the border – the multiple calculations and identifications that constitute the sovereign practices of authorization – that make the very idea of security possible. It is not the single declaration of exception per se that produces sovereign power, but the multiple “repetitive acts” that write the very possibility of a securable state (p. 301). Through interrupting these practices, they can be rendered strange and the repetitions on which they are based can be seen more carefully.

Analysing different artworks, Amoore and Hall highlight the ‘spaces of resistance that are always present in security practices’ (p. 301). For example, *Toy an Horse*, a ten metre high Janus-faced Trojan Horse placed at the border between Mexico and the US, defamiliarizes the border crossing through its presence and interrupts security sequences, potentially provoking a questioning of daily security practices. Another artwork, the *Transborder Immigrant Tool*, uses mobile phones equipped with GPS technology to indicate the safest and most aesthetic routes to pass the US-Mexican border through a Virtual Hiker algorithm. As such, it combines art and political act and temporarily reverses power by providing tracking technologies to those who are tracked. Finally, the art projects of Meghan Trainor use RFID (Radio Frequency Idenification) technology. The essence of Trainor’s work
is to experience RFID outside the contexts in which they are generally used and detaching them from pre-established meanings. These works have in common that they make the forgotten patterns on which security rests strange. They do not impose or demand judgement, but rather ‘discomfort and unsettle one’s sense of certainty’ (p. 312); they also stimulate public engagement by re-introducing the unexpected.

Like the border theatre of Amoore and Hall, the theatre of compliance is understood as a stage suggesting controllability through the repetition of mundane security practices. This chapter considers how the theatre of compliance brings into being groups and categories by analysing the ‘actors’ appearing on the stage. Drawing attention to the script and scenario of the theatre of compliance, the chapter analyses the ‘multiple repetitive acts’ through which financial (ab)normalities and (ir)regularities are identified, established and developed. In order words, it explores how the risk-based approach works on a day-to-day level in banking practice, and how categories of suspicion and abnormality are constituted through mundane acts of repetition, rather than strictly through overarching and fixed risk classifications. Unlike the work of Amoore and Hall, this chapter will not consider how artworks may draw attention to and question security practices by interrupting them, but it does aim to provoke reflection on security practices within banks by making them more visible through detailed description.

The risk of using theatre as a metaphor is its connotation of being something that is false or consisting of only appearance. I certainly do not want to suggest that compliance with the Directive by banks is anything but sincere. My experience from a range of interviews is that banks take implementation of the Directive extremely seriously and feel it is important to implement the law correctly. What the theatre of compliance metaphor makes clear is that the professional field and professional practices are in motion, and have grown enormously in recent years. The metaphor also aims to make to make visible a disconnect between the objective of the Directive – combating terrorism finance – and the shift that takes place while implementing the Directive – complying with CFT requirements. As will become clear below, these two objectives do not overlap, which makes a study of the political and societal implications of these measures all the more urgent.
6.4 The Stage

Within political science literature, the notion of the stage has been used for various purposes and especially in relation to the nation (state) (e.g. Hogan, 2003, Kruger, 1992, Wilmer, 2004). In these accounts the stage often refers to a site of ritual or self-representation. In this section, the notion of the stage permits consideration of actors belonging to the theatre beyond the institutional boundaries of the bank, and of the roles these actors hold as well as the different locations in which the play takes place. It shows how implementation of the Third Directive within banks is productive, like the theatre, as it brings into being a field of governing in which participants or actors contribute to ensuring compliance. In this section the stage undergoing analysis comprises the whole compliance process within a bank, from shaping CFT policies to reporting suspicious transactions.

To relate back to the professional field of the Third Directive presented in chapter 2, the examination of the stage resembles the mapping of a field of governance in that it makes different participants and the relations between them visible. However, the investigation of the stage in this chapter is restricted to the performing of compliance by banks, as opposed to the field map of chapter 2, which considers a broader transnational governing process. The stage described here consists mainly but not exclusively of the participants possessing operational powers on a national level represented in the lower right case of the field map.

Before analysing the different actors and sites of the theatre of compliance, it is important to stress that the stages of the theatre are different in every bank and form a very heterogeneous environment involving numerous and dispersed actors and sites within the bank. Despite the fact that one of the aims of the Third Directive is to harmonize AML/CFT requirements within and between EU member states, this does not imply that it imposes or provides a ‘one-size-fits-all’ model or a miracle solution for organizing compliance. A high degree of flexibility was indispensable for coping with the specificities of the different regulated professions, as well as the great diversity within specific professions. Banks differ with respect to their size, their core activities, their profile and their geographic presence, yet the Directive must be implemented by all banks, ranging from small savings banks to mainstream national retail banks and internationally operating commercial banks. Moreover, the various stages of compliance procedures take place in different locations within the bank, either in the front office or in the back office, at the local bank or national and international financial districts like the City of London.
However, it is possible to discern certain ‘actors’ and ‘roles’ that participate in ensuring compliance. At the core of a bank’s compliance policy are specialized back office departments, such as ‘Legal’, ‘Compliance’ and ‘Security and Intelligence’. These departments shape the bank’s compliance policy by developing procedures and processes, giving advice and monitoring. However, each bank designs its own organizational structure and may, for instance, decide to merge the Legal and Compliance departments. In addition, each bank makes its own decisions regarding the tasks of each department and the division of tasks between the front office and the back office. Bearing this in mind, the tasks of these three departments can be described as follows.

The Legal Affairs department interprets the law at the most abstract level. When, for example, the FATF (Financial Action Task Force) requirements, the EU’s Third Directive and the national AML/CFT law differ slightly on certain definitions, the Legal department interprets these differences and tries to correctly adapt the bank’s compliance policy (interview 16). The Legal Affairs department also gives legal advice with respect to specific clients or practices. For instance, a local office of a bank may ask advice about whether: ‘a Dutch bank can accept a Spanish bullfighter as a client when bullfighting is legal in parts of Spain but illegal in the Netherlands’ (interview 16).

The Compliance department translates legal requirements into internal CFT procedures and automated processes. They assess if products, processes or procedures are compliant with the law. To be more precise, this department develops, for example, the procedures for carrying out due diligence in accepting new clients. This department may also provide independent but non-binding advice in response to queries from the front office, for instance with respect to clients labelled as ‘high risk’. Another task that is sometimes taken up by Compliance departments is monitoring the implementation of advice and guidelines within the bank.

The Security and Intelligence department analyses risks with regard to products, clients and countries. They assess whether risk indicators and scenarios operating in risk analysis software need to be changed, and if new criteria need to be added. This work is done on the basis of a range of information, which includes newspaper articles, Internet searches, reports of NGOs, governments and international organizations, guidelines published by (inter)national bodies and internal data held by banks.

The front office or ‘business’ is the primary agent responsible for the application of the CFT policy. When a new client, whether an individual or a multinational company, presents itself at a bank, account managers and money-laundering reporting officers
MLRO’s) carry out the due diligence procedures set out by the Compliance department. Once the client is accepted, they are also responsible for monitoring their client’s transactions and for periodical review of the client. At each stage, risk assessments are carried out and clients or transactions are assessed as being low/normal risk or high risk. ‘Business’ interacts with and can ask for assistance of the Legal and Compliance departments.

When account managers and MLRO’s have suspicions with regard to a client or a transaction, they usually report this transaction internally and ask for advice from the Compliance department, which may in some cases even lead to direct involvement of the board of governors of the bank (interview 14). If further investigation leads to confirmation of the suspicion, the relevant department within a bank, often the Compliance or the Security and Intelligence department, may decide to send a suspicious transaction report (STR) to the national FIU. Such units are responsible for investigating the STRs and for taking further judicial action if needed. Furthermore, FIUs may also exchange information on suspicious transactions with FIUs in other countries, for instance, through FIUnet, a platform for enhanced cooperation between European FIUs sponsored by the European Union, or the Egmond Secure Web, an initiative from the Egmond Group of FIUs that fosters cooperation between FIUs worldwide.

In addition, national supervisory authorities such as Central Banks or national Financial Services Authorities evaluate and ensure compliance. Financial Authorities regularly visit banks or request information to assess (on a risk-sensitive basis) whether regulated entities have correctly implemented and executed (specific aspects of) the AML/CFT law. In the Third Directive, particular attention is given to the supervision of compliance, and it also introduces a section on penalties in case of non-compliance (Van den Broek, 2011a, p. 177). The EU-wide introduction of minimum standards for enforcement of compliance illustrates the seriousness of the theatre. Depending on national legislation and the nature of the infringement, sanctions may include a warning, blacklisting of compliance officers, or a fine. This last was the case for the Royal Bank of Scotland, which received a fine of £750,000 from the British Financial Services Authority for breaching AML/CFT rules (Financial Services Authority, 2002). Although it can be disputed whether the amount of the fee is dissuasive for a bank like RBS, the reputational damage to the bank has resonated throughout the international financial sector.

Finally, two more actors can be identified: banking customers and, in line with the previous chapter, the producers of due diligence software, as well as the software itself. While the transactional and personal data of customers are at the core of the AML/CFT compliance
policy, customers have only a marginal or ‘walk-on part’ in the theatre of compliance. Apart from delivering input to the compliance apparatus in the form of transactions or newly requested services, customers do not play a role. In fact, they are not supposed to be aware of the compliance procedures. Hindrance of ‘normal’ financial behaviour by identification and monitoring procedures should be minimized, while suspicious transactions and clients are to be silently flagged within the system of the bank or reported to the national FIU. In this latter case, the Third Directive, like its predecessors, explicitly prohibits informing the customer. With regard to the software used for monitoring transactions, the products developed by companies such as Fiserv, Bloomberg, Dow Jones and Wordcheck have become essential to being compliant with AML/CFT legislation. As discussed in the following sections, the design of these products influences the script and the performances within the theatre of compliance.

Considering all the different actors populating the stage, it may be noted that the numbers of actors involved can vary enormously according to context. A small savings bank may have only one or two persons responsible for compliance and legal issues (interview 20). The main office may be located in a stately home in a medium sized provincial town. At big international banks, on the other hand, each of the three back office departments may consist of 60 to 80 people (interviews 14, 16) working in big open-space offices at the main office in the heart of a financial district. The number of employees involved in AML/CFT-related tasks rises to between 500 and 1000 when including all the local branches of big banks, and often over 2000 when one takes into account internal auditors and tasks related to risk management (Favarel-Garrigues et al., 2009, p. 8). Likewise, the numbers of staff that analyse STRs within a FIU strongly differ. To give an impression of the differences, according to a 2005 IMF report the FIU of Slovenia employs 17 persons while 120 persons work for the British FIU (IMF, 2004, p. 12, 15). In 2008 the FIU in France employs approximately 70 persons (interview 5, see also Favarel-Garrigues et al., 2008), in the Netherlands 60 persons (interview 2) and that of Malta only four persons.39

While in the past banks have been reluctant to enforce AML compliance policies strictly, their attitude has changed over the last decade, especially since 9/11. Awareness that banks can be abused for terrorism financing or criminal activities is very high, and the commitment to defend the bank against this is very high too. Interviews with actors dealing with AML/CFT compliance within banks demonstrate that banks find it very important to be compliant. Many interviewees express a sincere concern about the damage terrorism and its financing do to society, and more importantly, the reputational risk of banks. They feel that
banks have a ‘moral obligation’ to fight terrorism financing and protect society (interviews 14, 16, 21). While some are sceptical about the efficiency of the Third Directive, all bank employees interviewed believe it is useful to have a barrier in place to make it more difficult to transfer money through the regular banking system. Moreover, it is highlighted that banks have no choice but to comply. Banks fear being publicly associated with terrorism, crime, dictators or other negative press since they are highly dependent on the public’s trust in their integrity. In the words of one bank employee: ‘you don’t want to open the morning newspaper reading on the front page that [your bank] is providing services to Osama Bin Laden or to President Mugabe’ (interview 14).

The cost of implementing the Third (and earlier) Directives and developing a compliance apparatus demands significant investment. This comprises not only the hire of specialized compliance officers, legal experts and security analysts, but also continuous staff training, the occasionally reliance on external expertise, and investment(s) in risk analysis and due diligence software. These software packages, which provide, for instance, data on blacklisted people and PEP’s, may ‘cost around 15,000 Euros per package’ (interview 21). Another estimate is provided by the British Banking Association: they believe that the overall annual cost of compliance with AML/CFT regulations is £36 million per individual institution (House of Lords, 2009a, p. 21). Yet it is difficult to assess the total costs and benefits of compliance with the Third Directive with any exactitude. Some interviewees estimate that the costs are ‘really enormous, and the (unintended) benefits, in terms of increased knowledge of customers and hence better marketing opportunities, are only marginal’ (interview 14). Others believe that ‘it is hard to assess but it might be the case that commercial benefits are equal to the additional costs of compliance’ (interview 17).

To conclude, the analysis of the stage shows that decision-making or, more generally, the exercise of power is dispersed over a range of actors across the public (FIUs, supervisory authorities) and the private sectors (banks). Further fragmentation takes place within institutions, such as the banks, and over different geographic locations. Moreover, the number of actors involved, their roles, their location, and the costs of compliance differ for each bank. This means that compliance with the Third Directive and other national and international CFT guidelines, gives rise to a field of governing in which participants have very specifically assigned responsibilities and powers that are however, non-transparent and difficult to assess by outsiders.
6.5 Script and Scenarios

Despite the variety of ‘stages’ on which AML/CFT compliance takes place, there is one common ‘script’ for being compliant set out in the Third Directive. This script consists of the Customer Due Diligence (CDD) procedures and practices that have been developed as part of the bank’s internal risk-based AML/CFT compliance policy. One aspect of the script is the use of scenarios, for instance those proposed by the FATF, against which transaction patterns are matched through the use of specialized software. An examination of the script and scenarios used for complying with counter-terrorism financing legislation highlights how assumptions about terrorism financing are translated into techniques of governing, and draws attention to the philosophy underpinning the governing of the fight against terrorism financing. For analytical purposes, the script (hence CDD) can be divided into two parts. The first concerns customer identification procedures that must be carried out when accepting or periodically reviewing a client. The second part of the script deals with transaction monitoring, which is a continuous activity. Both parts are structured by the risk-based approach introduced in the Third Directive.

6.5.1 Customer Due Diligence Part One: Customer Identification

In the First and Second Directives, the ‘Know Your Customer’ (KYC) principle was a central element. According to this principle, banks and other institutions in the financial services sector were required to know the identity of their customers and their transactions. This implies that they have ‘the duty to identify their customers and the corollary duty to keep records of identification and transactions’ (Mitsilegas, 2003, p. 69). In the Third Directive KYC has been replaced by more detailed and differentiated identification requirements under the notion of Customer Due Diligence (CDD).

Originally, due diligence was undertaken in case of corporate mergers and acquisitions. It entails a practice ‘through which the parties to a merger spend time checking the balance sheets and legal histories of their potential partners before closing the deal’ (Maurer, 2005, p. 476). These practices have also been introduced in offshore finance, where they involve ‘checking the details of a person’s or corporation’s identities against potential wrongdoing’ (ibid.). This same definition can be used for customer due-diligence procedures for the purpose of combating the financing of terrorism.
At the start of a business relationship, CDD procedures consist of information gathering via a face-to-face or telephone conversation on basis of a standardized questionnaire or an (online) application form. One objective of this procedure is to find out the purpose and the intended nature of the business relationship with the customer. It enables the bank to ‘predict with relative certainty the types of transactions in which the customer is likely to engage’. Of course we also learn a lot from this and there are commercial advantages of knowing your customer’ (interview 14). However, the CDD procedures do not appear to be an efficient preventive tool when it comes to uncovering new terrorists as yet unknown. Despite questions about the client’s intentions in opening a bank account, it is very unlikely that a terrorist will reveal his plans. As mentioned by a bank employee ‘of course a terrorist will not indicate that he wishes to open a savings account to save for explosives’ (interview 16).

Another objective is to establish the client’s identity or the beneficial owner of a company on basis of a reliable and independent source (Handoll, 2006, p. 153). The required documents for this differ among EU member states. For instance, the UK does not (yet) have an ID-card, while in most other European countries, a copy of an ID-card is required for opening an account or passing financial transactions. However, even when ID cards are used, these may be false or the translation of the identity of the consumer from another alphabet can provoke confusion. ‘Focussing on names is difficult as the translation from Arabic into European letters often leads to different ways of spelling a name’ (interviews 2, 20). It happens that ‘the database stores data of one and the same person under 14 different spellings’ (interview 2). In the case of companies, proof of registration with the Chamber of Commerce is often requested to establish the legal identity of the company. A risk assessment is carried out on the basis of the information provided and the customer data are also automatically matched against various blacklists.

In the case of combating terrorism financing, the most important blacklists are the UN, EU and national ‘terrorist lists’. The occurrence of a match against these lists should prohibit banks from doing any business with the client. However, interviewees confirm that hits against the terrorist lists hardly ever occur. Those mentioned on the list will simply not attempt to do any business with banks themselves or will assume a false identity. Concerning terrorists that have not yet been identified, these lists will obviously not be of use, as their names will not be included. Hence, in addition to the many important problematic aspects of blacklisting raised by legal scholars, notably with regard to due process and the international legal framework (i.a. Guild, 2008, 2010), one may ponder the implications of having to check all clients against lists while never provoking a hit.
Subsequently, clients are labelled as either low/normal risk or high risk through a system of points calculated by risk-analysis software (interviews 14, 15). An individual can for instance be labelled high risk when his or her name matches a name on Worldcheck’s database of Politically Exposed Persons (PEP), worth 75 points. As mentioned above, all foreign political, military and judicial leaders and their inner circles are to be considered PEPs. Usually these people are not terrorists, but they may also have a link to terrorism, be involved in corruption or engage in organised crime. It is, however, not forbidden to accept them as a client. Moreover, it is possible for a client to be considered a PEP at one bank and not another, because ‘the PEP software packages sold by for instance Bloomsberg or Dow Jones do not contain the same names and banks may also add new PEPs to their monitoring system’ (interview 17).

Labels are also assigned on the basis of the products used by the client. Opening a savings account, for instance, is considered low risk and is worth zero points. Companies might be indicated as high risk when they do business with high-risk countries. For illustration, an internal document of an international bank shows that (at least in one particular instance) this bank considered 69 countries as being high risk, while only 19 countries, of which only 9 are EU member states, were considered low risk (tables 6.3 and 6.4). This means that a slightly higher risk score is attached to transactions involving one or more of the 18 medium risk EU member states. Companies are also assessed according to their sector of activity. According to internal documents of this same bank, an agricultural firm is for instance rated at zero points; a convenience store rates 30 points and a money services business 75. On basis of the scores on these and other criteria, a score is calculated defining whether the client represents a low or a high risk.

However, the assumptions underpinning the risk-based approach are problematic in some respects. Although the attribution of these risk scores provides a semblance of support for the calculability of terrorism financing risks, the detection of potential terrorist financiers by means of risk analysis entirely depends on the assumption that terrorists display behaviour different from other customers. However, it has not been proven that this is actually the case. Consequently, it means that if terrorists and their financiers do not display different behaviour they will never be detected. In the words of a representative of the banking sector ‘if a yet unknown terrorist opens a savings account at our bank we will probably not detect this because it does not differ from something you and I could do’ (interview 27).
### High Risk Country List

The following countries are considered high risk by one London bank, and therefore, any direct or indirect relationship a customer of this bank has with any of these countries must be noted in the Customer Due Diligence Questionnaire.

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>East Timor</td>
<td>Lebanon</td>
<td>Sao Tome Principe</td>
</tr>
<tr>
<td>Angola</td>
<td>Ecuador</td>
<td>Liberia</td>
<td>Serbia</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>Equatorial Guinea</td>
<td>Libya</td>
<td>Sierra Leone</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Eritrea</td>
<td>Macedonia</td>
<td>Solomon Islands</td>
</tr>
<tr>
<td>Belarus</td>
<td>Ethiopia</td>
<td>Malawi</td>
<td>Somalia</td>
</tr>
<tr>
<td>Bolivia</td>
<td>Gabon</td>
<td>Maldives</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Bosnia-Herzegovina</td>
<td>Gambia</td>
<td>Mongolia</td>
<td>Sudan</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>Guinea</td>
<td>Montenegro</td>
<td>Syria</td>
</tr>
<tr>
<td>Burundi</td>
<td>Guinea-Bissau</td>
<td>Myanmar (Burma)</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>Cambodia</td>
<td>Guyana</td>
<td>Nepal</td>
<td>Togo</td>
</tr>
<tr>
<td>Cameroon</td>
<td>Haiti</td>
<td>Nicaragua</td>
<td>Turkmenistan</td>
</tr>
<tr>
<td>Central African Republic</td>
<td>Iran</td>
<td>Niger</td>
<td>Uganda</td>
</tr>
<tr>
<td>Chad</td>
<td>Iraq</td>
<td>North Korea</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>Comoros</td>
<td>Ivory Coast</td>
<td>Pakistan</td>
<td>Venezuela</td>
</tr>
<tr>
<td>Cuba</td>
<td>Kazakhstan</td>
<td>Palestine</td>
<td>Yemen</td>
</tr>
<tr>
<td>Democratic Republic of Congo</td>
<td>Kenya</td>
<td>Papua New Guinea</td>
<td>Zambia</td>
</tr>
<tr>
<td></td>
<td>Kyrgyzstan</td>
<td>Republic of Congo</td>
<td>Zimbabwe</td>
</tr>
<tr>
<td></td>
<td>Laos</td>
<td>Rwanda</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.3 Source: Internal Memorandum, an internationally operating bank in London. (May 2010).

### Low Risk Country List

The following jurisdictions are considered low risk in the same bank.

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica</td>
<td>Denmark</td>
<td>Netherlands</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Australia</td>
<td>Finland</td>
<td>New Zealand</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Austria</td>
<td>France</td>
<td>Norway</td>
<td>United States</td>
</tr>
<tr>
<td>Belgium</td>
<td>Iceland</td>
<td>Singapore</td>
<td>Vatican City</td>
</tr>
<tr>
<td>Canada</td>
<td>Luxembourg</td>
<td>Sweden</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.4 Source: Internal Memorandum, an internationally operating bank in London. (May 2010).

Furthermore, the level of risk given to a transaction or client is not simply the outcome of an objective computerized risk assessment. The number of points assigned to each product, country or sector of activity, and on which the risk calculations are based, are defined by banks themselves and they can be modified. Moreover, ‘there is quite some room for manoeuvre within the definitions of the law. Which means that compliance officers have to make choices on how they appreciate a situation’ (interview 9). High risk scores, for instance, do not automatically lead to reporting to an FIU or the closure of a business relationship. In practice, it is possible and happens that customers are labelled high risk and they are not rejected. As long as it is not strictly forbidden by law to do business with a specific customer, it is seen as part of the ‘commercial freedom’ of a bank to either accept or reject a customer. While these risk calculations remain attached to the client’s file, and past risk flags always
remain visible, bank personnel have some discretion to judge these risks themselves and may decide to ignore high-risk flags, or to scale clients back from high risk to normal risk.

On the other hand, banks and financial services providers may also decide not to engage in business activities with individuals or businesses for other reasons than official blacklisting or high-risk scores according to established risk criteria. For instance, in 2010, Bank of America, Visa, MasterCard, Western Union and PayPal decided preventively to refuse all payments to Wikileaks (Arthur, 2012). Another example is the refusal of two Dutch banks, Rabobank and ABN AMRO, to open an account for Marthijn Uittenbogaard, a publicly known advocate for the acceptance of paedophilia (Heijne, 2012). Hence, the due diligence procedure as a whole, and risk assessments in particular create a grey zone in which banks themselves ‘can decide how tough they want to be on certain criteria [of the compliance policy]’ (interview 14) and which considerations in addition to those specified in the Third Directive they take into account.

This implies that risk analysis does not reflect an objective reality, but depends on the interplay between the officer assessing flagged transactions or customers and the compliance software. A hearing on money laundering and terrorism financing before the select committee on the EU of the House of Lords is very insightful in this respect and is worth quoting at length. In response to the question on what basis suspicious transactions are to be reported, the Deputy Chief Executive of the British Bankers’ Association stated:

(…) it is a suspicion based regime. (…) You rely on your instincts; you have the framework of the law; you have the framework of the banks’ own methodology for assessing risks, whether it is the type of customer or the product they are taking, or the country in which they are situated, and that is the suspicion, it is the experience of the person concerned that triggers that (2009a, pp. 26-27).

Responding to the question on whether reports can be made ‘on that feeling’, she responded,

Absolutely; you are required to, that is what the law requires (…) We have to. The law requires that if you suspect you must report (ibid., p. 27).

These responses not only highlight the involvement of human considerations as part of risk analysis, but they also emphasize the need for bank employees to share the norms and ethical standards of the bank and make their decisions accordingly. ‘The risk-based approach requires discipline and confidence in your employees [making the security decisions] because [the bank] counts on their opinion, your objectivity’ (interview 14).

This analysis of the customer due diligence procedures undertaken at the start of, or during, a business relationship with a client shows that, much like border security, these consist of
multiple repetitive and protocolled acts of ‘scanning, screening and verification’. However, the detailed description of these acts to ensure compliance shows that the risk-based approach is not merely a simple and straightforward calculation of risk-scores. In order to know the customer, a significant portion of the CDD procedures rests on a subjective estimation and weighting of information regarding the customer’s identity and intentions. Hence, despite the apparent objectivity of the calculation of risk scores, subjectivity is an important aspect of the risk-based approach, because personal conviction, professional instincts and knowledge about terrorism financing partly influence the assignment of risk scores and the consequences of these scores.

6.5.2 Customer Due Diligence Part Two: Transaction Monitoring

In addition to the procedures concerning the acceptance of new clients, the continuous monitoring of customer transactions is another important part of the script of the theatre of compliance. Currently the banking industry passes through 550 transactions a second (House of Lords, 2009a, p. 14). To monitor all these transactions on a risk-based basis implies that ‘during the night a bank’s computer system matches enormous datasets with thousands of customer requests each day, against a number of detection, monitoring and filtering systems’ (interview 14). The continuous risk assessment of customers’ transactions is a very similar process to the initial risk assessment that is part of the customer identification procedures. Different aspects of a financial transaction are translated into risk criteria and are given a certain number of points. Depending on the total number of points, a transaction may emerge as ‘risky’ or ‘requiring further attention’ on the computer screen of a Money Laundering Reporting Officer or an account manager. On average, 2% of all transactions produce a hit in the system and require further attention, meaning that the customer is asked to provide additional information, which is then recorded in the system.

One of the difficulties of detecting terrorism financing through the risk assessment of transactions is the modest and strongly decreasing cost of an attack. The risk-based approach entails checking the amount of each transaction; transactions above a certain amount will provoke a hit in the system. The Third Directive, for instance, prescribes that transactions above € 15,000 are to be considered risky. However, the estimated cost of the 2004 Madrid attacks was only € 10,000, and costs for the 2005 attacks in London were only one tenth of that amount. Furthermore, these funds were raised completely through legal means such as salary and savings money (Buchanan, 2006).42 ‘These amounts cannot be detected unless you
allow for screening everyone’s expenses up to a few Euros at the local groceries store. It does not work’ (interview 15).

Aside from assessing transactions against specific risk criteria, all transactions of each client are also checked against scenarios. This means that:

certain patterns are expected. Especially with regard to private customers, 95% of them have the following pattern: at the end of the month money comes in, on the first day of the month rent or mortgage, gas, electricity and insurance bills are paid and the rest is used for consumption and perhaps savings and an occasional holiday. This is considered as a normal process (interview 14).

A fully automated process is run by specialized risk monitoring software such as ERASE, a program developed by a Dutch company NetEcology, one of the market leaders in this sector and since 2007 part of the American company Fiserv. There are also specific scenarios for businesses. A normal pattern for a bakery is to make regular purchases of flour and eggs, for instance, and to earn income within a certain range. If a bakery suddenly has an enormous increase in income or requests services that do not correspond with its business, this can provoke a hit or red flag in the system.

While the object of risk assessments involving specific criteria and scenarios is to enhance control over financial transactions, it must be emphasized that they also entail a vision of how a customer’s ‘normal’ financial life should look. When customers correspond to the scenario, their transactions pass unnoticed through the system. If their transactions differ from the scenario, a ‘risk flag’ or a ‘hit’ is produced. This is for instance the case ‘when suddenly receiving three times 17,000 Euro in four weeks’ (interview 14) or when ‘suddenly receiving 50,000 dollars from an account in the US’ (interview 17). Or ‘when we see that money comes in several times a month or we see that transactions are made to foreign countries, frequent cash transactions or rapid movements of funds, these are not normal for an average household’ (interview 14).

On the basis of reports by international organizations such as the FATF, the World Bank and the IMF, commercial companies have also developed specific scenarios for detecting terrorist funding. However, banks seem sceptical about these scenarios. ‘We [automatically] check against the proposed scenarios but there are no hits’. ‘Moreover it is impossible to make scenarios of terrorists because every attack is different. There is no profile of a terrorist’ (interview 14). The FATF also acknowledges that the diversity and multifaceted nature of terrorists’ financial activity makes it challenging to establish general alerts and indicators that suggest a particular transaction presents a risk of terrorist finance. They do, however, propose that large cash or electronic transfers and cross-border currency
transactions might be signs of terrorism financing (FATF, 2008, p. 29). Other indicators that are often found in revealing terrorism financing cases are the sending or reception of funds by international transfer from or to locations of specific concern, atypical business or account behaviour, transactions linked to a charity organisation, large scale cash transactions, and media coverage of account holder’s activities (ibid., p. 31).

When a hit occurs and a transaction is considered suspicious, banks fill out a suspicious transaction report (STR) indicating the characteristics of the transaction (sender, beneficiary, currency, amount…) and the type of suspicion, which is sent (electronically) to the national FIU. At this moment, the transaction moves from the private sector to the public sector. The FIU stores the STRs it receives in a huge database. In countries such as the UK and the Netherlands, the number of STRs received daily by the FIU exceeds their capacity to analyse. ‘It is impossible to look at all STRs’ (interview 2). Subsequently, officers of the FIU investigate STRs that are flagged on a risk-sensitive basis similar to the approach adopted by banks. ‘We make lists of risk criteria, to detect terrorism, for instance, it is important to look which countries are involved, and the STRs that receive most points on basis of the risk assessment are investigated’ (ibid.).

However, cooperation between the public and private sectors goes beyond the mere reporting of suspicious transactions. The FATF encourages banks and FIUs to regularly exchange information on terrorism financing. Specific cases or trends found in the financial intelligence gathered by FIUs could provide clues for the terrorism financing scenarios that are developed by banks themselves, while banks could give feedback on the results obtained from the scenarios suggested by a FIU (FATF, 2008). However, this cooperation is still to be developed. Although the EU Financial Intelligence Unit Platform has dedicated attention to this issue (EU Financial Intelligence Unit Platform, 2008) and some FIUs have started to strengthen their relations with reporting entities, bank employees stress the lack of feedback they receive regarding the STRs they send to the national FIU (interview 2). In the UK, the Serious Organised Crime Agency (SOCA) has increasingly provided feedback to banks and other reporting entities with regard to the reports they have made and new trends that have been observed. However, so far, reporting entities are qualifying the feedback as ‘not very helpful in that they are too general’ and claiming that it ‘tends to confirm what the industry already knows’ (House of Lords, 2009a, pp. 30-31).

Moreover, while the lack of terrorism financing hits might be understood as reassuring news about the threat of terrorism to our society and the integrity and soundness of the financial system, it does create a little unease within some banks. It leads to what has been
called ‘defensive reporting’ which the risk-based approach aimed to avoid by introducing more flexible reporting standards. If banks have doubts about a suspicion, they decide to report and be on the safe side of the law. Another reason banks report defensively is to satisfy monitoring authorities. According to a bank employee: ‘every year we send one or two “defensive reports” to the FIU’. ‘We know it is not a terrorism case but we do not want to mark zero detections in our statistics and if we report some they notice at least that we are not sleeping’ (interview 15). The British Bankers Association even explains that they have some sort of agreement with SOCA with regard to separating the wheat from the chaff in the STR reports that they send (House of Lords, 2009a).

In sum, examining the script and scenarios of the theatre of compliance makes the rationality of governing the fight against terrorism financing visible. Customer Due Diligence procedures prescribe how the customer must produce and represent him or herself to gain access to the formal financial system. Risk assessments and scenarios call into being certain ideal types of normal financial behaviour to which the financial lives of ordinary customers should correspond, and produce risk flags in response to suspicious or unusual transactions. The assumptions regarding what is potentially a sign of terrorism financing are strongly shaped by the FATF special recommendations on this topic, and are occasionally informed by financial intelligence from FIUs. These assumptions are integrated in a bank’s risk-analysis software and transaction scenarios and structure the fight against terrorism financing. In practice this means an increase of surveillance on citizens and businesses that make international transactions, that transfer money to charities, or that make large (cash) transactions. The quality and follow-up of decisions taken on the basis of these scripts and scenarios depend on the relations between public and private authorities. The adoption of the theatre metaphor and the examination of the practices of the Third Directive in terms of script and scenarios also draws attention to the subjective and controversial aspects embedded in these practices.

6.6 Performance

Performance can be defined in several manners. In conventional economic and financial analysis, performance is an important indicator. It usually intends to make the achievements of businesses or government agencies measurable, providing ‘a logic of calculability and an appearance of scientific objectivity’ (De Goede, 2005, p. 3). Such
indicators are, for example, customer satisfaction grades, rising stock prices, or numbers of received STRs. From this perspective, the performance of the Third Directive can be expressed in terms of effectiveness with regard to the objectives of the Directive.

Understood in reference to the theatre, performance has increasingly been used as a valuable concept in social and political analysis over the past two decades (Nield, 2006, p. 63). De Graaf (2010), for instance, assesses the performance of combating terrorism in different countries. In her study, performance does not refer to the effectiveness or success of counter-terrorism policies, but rather entails the presentation and perception of counter-terrorism measures. Performative power can be defined as the imaginative power and persuasiveness of a counter-terrorism policy and includes parameters such as agenda setting, public support and discourse (De Graaf, 2010, p. 139). Performative power is high when political and public opinion are strongly mobilized. This section examines the performance of the Third Directive from both the economic and the theatrical perspectives.

A first objective of the Third Directive is to detect terrorism financing and identify terrorists and their associates. The number of STRs falling under terrorism financing may offer a rough idea of the effectiveness of the Directive in combating terrorism (and of compliance with the Directive). It must be stressed, however, that the FIUs of EU member states do not always publish their statistics in comparable formats, they do not always indicate the number of reports related to terrorism financing separately; these numbers also include reports that do not lead to prosecution. For instance, the UK FIU, SOCA, reports that 247,601 Suspicious Activity Reports (SARs) were reported in 2011, of which 662 (less than 0.25%) were related to terrorism financing. Approximately 73% of all reports were filed by banks (SOCA, 2011, p. 52). The 2010 annual report of the Dutch FIU indicates that it received a total of 183,395 STRs in 2010 and notices that ‘with regard to the financing of terrorism several interesting cases have been shared with investigation [officers]’ (FIU-NL, 2010, p. 11). However, the report does not provide detailed numbers on terrorism financing as the Dutch Ministry of Finance has decided to suppress the box indicating a suspicion of terrorism from the STR form in 2005, to alleviate the administrative burden on reporting entities (interview 2). The French FIU, TRACFIN, notes that very few cases of terrorism financing are detected; 17 cases were transferred to the judicial authorities in 2007, 5 in 2008, 9 in 2009 and 6 in 2010 (TRACFIN, 2011). According to a representative of the Polish FIU, it had received only one STR in relation to terrorism financing within that year, and after investigation it appeared to be a false alert (EIPA, 2008). However, given the extremely low incidence of terrorist acts, it is difficult to conclude whether the few potential cases of
terrorism financing that are reported, and the sporadic prosecution on the basis of STRs are to be interpreted as a success or not.

The opinion of participants involved in reporting suspicious transactions on the performance of the Third Directive with regard to detecting and identifying terrorism financiers is rather more negative. According to one bank employee ‘it is a utopia to believe we can detect terrorists through transaction monitoring. This policy is symbolic, the person that holds the illusion that this works does not live on this planet’ (interview 14). In hearings before the House of Lords, the British Law Society and the British Banking Association expressed that they ‘continued to have concerns as to the effectiveness of the scheme’ (House of Lords, 2009a, p. 4). Also, FIUs are critical of the effectiveness of the system, especially due to the overload of information it creates. ‘What we attempt to do is not finding a needle in a hay stack but finding a needle in a stack of needles’ (interview 2). Similarly, on the level where guidelines and legal frameworks are designed, it is known that results are limited. EU officials do not appear to be convinced by the effectiveness of the Directive (interview 10). In a similar vein, a recent FATF report acknowledged ‘that financial institutions will probably be unable to detect terrorist financing as such’ (FATF, 2002, p. 3).

The other objectives of the Third Directive are even more difficult to assess quantitatively. As mentioned briefly in the introduction of this chapter, the deterrent effects of the Directive cannot be easily measured, as this implies counting terrorism-related transactions that did not take place (in the formal financial system). It is possible that the dissuasive effects of the Directive have resulted in a shift to other means of transferring or accumulating money outside those services and businesses subject to the Third Directive. In that case, the Directive has achieved its objective of denying terrorists access to the formal financial sector, but terrorists may still have access to alternative means of financing. On the other hand, it is possible that terrorist financiers continue to make use of banks and financial services but avoid detection by using false identities and leading financial lives that do not raise red flags.

Likewise, the more general objectives of the Third Directive, being the stability and reputation of the financial sector and confidence in the financial system, cannot easily be judged in terms of effectiveness. The number of terrorism related STRs does not reveal the total terrorism financing transactions that take place in the formal financial system and it is virtually impossible to know what percentage of terrorism transactions is intercepted. Moreover, it can be questioned whether the sums of money involved in financing terrorism would indeed suffice to destabilize the global financial system. In fact, similar to the point
raised by Nield (2006) with respect to the border, the Third Directive does not objectively regulate existing norms of integrity or reliability, but contributes to producing the idea of a sound and clean financial sector through the creation and performance of AML/CFT practices.

Considering the performance of the Third Directive in theatrical terms helps to explain why the theatre of compliance continues even when performance in economic terms is low or proves to be elusive. First, the monitoring and reporting requirements of the Third Directive are considered a barrier making it, in theory, more difficult for terrorists to gain access to the regular banking system. It is precisely the extensive and strict requirements, the establishment of public and private structures assessing suspicious transactions and the supervision of compliance that contribute to a belief in the control, integrity and soundness of the financial sector, irrespective of actual results. This also touches upon Schneier’s argument of the ‘security theatre’ in which counter-terrorism policies aim to reassure the population.

At the level of banks, respecting AML/CFT regulations and maintaining good relations with supervising authorities are part of the communication strategy for presenting the bank as trustworthy and solid. Banks have invested heavily in being compliant and want to avoid reputational damage at virtually any cost. According to Tsingou, the largest global financial players even have a business interest in maintaining the status quo, as they helped shape the current standard that ‘affects small institutions disproportionately,’ as their means to make the required investments in compliance are more limited (2010, p. 183). In addition, banks seem to derive at least some benefit from the CFT requirements, as better knowledge of their customers generates additional marketing opportunities.

Already twenty years ago, banks such as the American Citibank understood the business opportunities of, at that time, Know Your Customer information. For instance, through transaction monitoring banks may notice that you inherited $50,000 and they can commercially anticipate on that by advising you what to do with this money (interview 17).

Hence, from a broader economic perspective, the theatre of compliance is also a power struggle of big banks and smaller ones, and it increases the power of banks over their customers.

Finally, there is a question of audience. The above may suggest that one of the audiences of the theatre of compliance is constituted by the supervising authorities that evaluate banks’ performance. The efforts banks undertake for being CFT compliant need to satisfy supervising authorities. However, supervising authorities can also be considered part
of the theatrical performance, in the sense that their opinion may (or may not) convey credibility and legitimacy to banks. From a broader societal perspective, the theatre of compliance is performed for the population, and increasing their feelings of security and their confidence in the current financial system. In this light, it is interesting to notice that this audience has no access to the stage, the script and the scenarios as described in this chapter. They cannot watch how CFT compliance is carried out, but it is crucial that the performance, in economic and in theatre terms, is convincing to them. The final section recapitulates how the Third Directive has created a new professional field, sets in motion new governing practices and addresses their implications.

6.7 Conclusion

The theatre of compliance metaphor offers a new and important approach for examining the daily governing practices that have been created to implement the Third Directive. It provides insights in the way public and private authorities cooperate to combat terrorism financing, in risk-based financial surveillance practices and the often overlooked implications of these new forms of governing.

The analysis of the stage of the theatre shows that the professional field which has emerged from the risk-based implementation of the Third Directive consists of both private and public authorities. Private actors, most notably banks, identify risky clients and monitor suspicious transactions, while public authorities either act upon the information delivered by the private sector or supervise the implementation of the Directive. The division of roles among the participants of the field and the design of the stage are of great importance. In daily practice, it means that a range of private professionals (developers of detection software, compliance officers within banks, legal experts...) are responsible for the filtering and pre-selection of the risky profiles and transactions through an accumulation of individual and fragmented decisions. Subsequently, these decisions structure the investigations led by FIUs and eventually the prosecution of terrorism financers. Hence, by charging banks with the responsibility to combat terrorism financing, a shift has taken place as banks are now involved in national security questions and are even the first to make certain security decisions.

Moreover, the analysis through the theatre metaphor has also shown that it not indifferent whether the public or the private sector is responsible for combating terrorism. Although the argument that the private sector can combat terrorism financing more efficiently
and more cheaply on the grounds that it already possesses financial data has some legitimacy, it needs to be emphasized that a bank’s primary mission is not combating terrorism financing. While banks claim to feel a social and moral commitment with respect to combating terrorism financing, their first reflex is to not act as ‘unpaid criminal investigators’ (interview 14). In practice, this leads to a discrepancy between the Directive’s objective of combating terrorism financing and the banks’ objective of being compliant with CFT measures and calls the effectiveness of involvement of the private sector into question.

Furthermore, the responsibility of the private sector to detect suspicious clients and transactions and the diffused decision-making procedures across multiple departments within institutions lead to an almost complete lack of transparency and accountability. In the words of a representative of the British Banking Association: ‘there is a risk to the risk-based approach itself in that it does mean that banks have to make judgements, people have to take responsibility (…)’ (House of Lords, 2009a, p. 25). So far it is unclear to outsiders when decisions are taken and on the basis of what information. As the monitoring and reporting process are and must be entirely hidden to clients it is impossible for them to control, complain or appeal against a bank’s decisions. Yet, the fact that defensive reporting of fictive suspicious transactions takes place and may lead to erroneous inclusion in police databases makes the case for accountability all the more urgent.

The risk-based approach introduced in the Third Directive also gave rise to a mode of governing terrorism financing through supposedly objective and scientific calculations. Through the daily repetitive acts of matching profiles against watch lists, calculating risk scores and monitoring transaction scenarios and with the help of ‘smart’ software programmes, security is enforced and the future appears manageable. However, an analysis of the Third Directive from the theatre of compliance perspective destabilizes the idea of the risk-based approach as a neutral practice. It shows that the specific characteristics of this approach – mobile norms and high flexibility for implementation – are not uncontroversial.

The analysis of the script shows that risk analysis depends on the risk indicators that are themselves based on client and transaction information gathered by the bank, and on risk classifications produced by the bank or by specialized compliance software and consulting companies. Hence, risk analysis is not made according to some objective standard, but emerges from the information suitable for calculation, and from the subjective shared assumptions about terrorism financing (and other crimes) of the professional field. Moreover, decisions regarding the suspiciousness of transactions deemed risky and decisions to report transactions to the FIU are always made by human beings. As such, decisions about suspicion
and risk are in essence ethical and social rather than technological and mathematic. The risk-based approach relies strongly on the subjectivity of the participants of the field and the institutions they represent. Security decisions are taken on the basis of their experience and knowledge, which is partly based on international guidelines. This again means that security decisions taken within banks are rather opaque and can be controversial, as for example when similar cases might be treated differently by different banks or bank employees (interview 9).

Another principal characteristic of the risk-based approach is the flexibility of norms and practices to combat terrorism financing. Flexibility is, on the one hand, justified by the fact that the modus operandi of terrorists may continuously change, and the Third Directive covers a wide range of professions within which a great variety may also exist. Yet, the downside of the mobile norms and flexible implementation of the risk-based approach is that it introduces legal uncertainty and lacks transparency. The fact that, within the limits of the law, each bank can define its own compliance policy and makes its own risk assessments, makes it unclear how exactly banks monitor their clients, what criteria they have developed for assessing their customers, and how strictly they enforce these criteria. It can even lead to discrimination as compliance officers are supposed to make their decisions on their intuition and personal expertise. Moreover, customers (must) remain almost entirely uninformed about the fact that their data are continuously assessed and might be reported to Financial Intelligence Units without their being notified.

The shortcomings of the risk-based approach – lack of transparency and accountability – are important in the light of the finding that the Third Directive has a theatrical function in reassuring citizens and financial markets but is not well suited to combating terrorism financing. In fact, detecting terrorism financing through the monitoring of clients and transactions is very complicated. The cost of terrorist acts is relatively low and decreasing, the financing of an attack does not necessarily require atypical financial behaviour and the occurrence of terrorist acts is too rare and similarities between the methods of financing are too low to establish meaningful scenarios.

Finally, the findings of this chapter, as well as those of previous chapters, start from the basis of governance practices and new professional fields that have emerged in the name of the European fight against terrorism financing. In the next and concluding chapter, the findings of the two case studies will be discussed in relation to the broader academic debate over financial surveillance in Europe. Are the practices of the Third Directive and the TFTP best understood as examples of financial surveillance, as suggested by certain scholars? Moreover, both cases have shown that these new governance practices lead to a variety of not
only legal but also political and societal questions. The final chapter also discusses the extent to which the (financial) surveillance prism can make these wider implications of the fight against terrorism financing visible.