Policing the Money: Compliance and AML in Belgian Banks[1]

Antoinette Verhage[2]

1. Introduction

As is commonly known, the battle against money laundering emerged in the late 80s of the previous century (Levi, 2002), first in the US, to catch on in Europe in the early 90s. As a result of the attention for this type of crime, a preventive and repressive system was built, including both public and private partners. Between then and now, 3 European Directives have governed the way in which money laundering should be tackled[3].

These European Directives have currently all been implemented in Belgian law[4], which has had several results. First of all, the Directives made clear that a preventive approach was necessary to combat money laundering. The repressive approach, characterized by criminal investigations in which 'following the money' became central, was not sufficient in the battle against money laundering.

Second, this preventive approach is built on the detection and reporting of suspicious transactions. It implies the engagement of a large number of public and private (over 58.000[5]) actors – of a large diversity, such as lawyers, notaries, exchange offices, guarding companies and financial institutions. These actors (both individuals and organisations) are required to report each potentially suspicious transaction or client to a central reporting unit, the Financial Intelligence Unit (or FIU). The FIU subsequently investigates these reports and decides whether or not they should be sent to the Public Prosecutor. The main task of the Belgian FIU is to gather information and analyse this in view of the battle against money laundering. They are bound by a strict professional secrecy which makes information exchange very limitedThis chain of events and actors is what we have called in our study the **anti money laundering (AML) chain**.

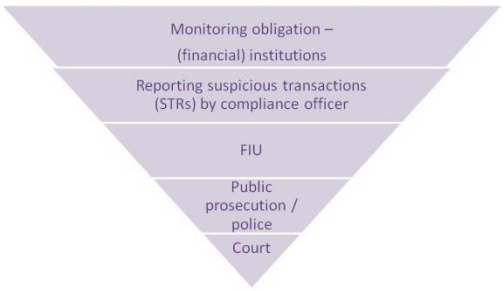

Figure 1 the AML chain

This reporting duty on the first level of the chain requires a thorough insight in clients and transactions. It implies that organisations are able to recognize suspicious transactions from non-suspicious transactions. It also entails that organisations need to invest in the battle against money laundering, in order to develop skills, instruments and

[1] This paper is an amended version of "VERHAGE, A., (2012), The social analysis of the anti money laundering complex and the compliance industry. In: PONSAERS, P. (ed), Social Analysis of Security, Boom, Groene Gras, Den Haag, 2012.

[2] Post-doc researcher, Department of Penal Law and Criminology, director Director Institute for Urban Security & Policing Studies (SVA), Chief Editor of the European Journal of Policing Studies, Faculty of Law, Ghent University.

[3] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; Directive 2001/97/EC of the European Parliament and Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering; and Directive 91/308/EEC of the Council of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

[4] Although it took Belgium until January 2010 to implement the 3rd Directive (while the deadline for implementation was set on 17 December 2007).

[5] Information provided by the Belgian FIU, March 4, 2011

competences that should allow them to detect potential money launderers and people related to terrorist activities.

The financial sector, also triggered by a number of other impetuses (such as their reputation protection), has been given a specific place in this amalgam of reporting actors. The financial sector is crucial in its control of the entrance into the world of the formal economy but is also very vulnerable (reputation wise) for abuses of their systems. This explains why the financial regulator (CBFA in Belgium) was the first to compel the financial sector to install a new function, partly dedicated to fighting money laundering: the compliance officer. As from 2001, each and every Belgian bank is obliged to have at least one compliance officer in its ranks (CBFA, 2001b). This compliance officer is responsible for the general 'integrity' of banking and therefore has AML and preventing terrorism financing as 'just' one of his/her tasks (CBFA, 2001a). After imposing this obligation, the regulator has also developed regulation concerning the (minimal) expectations for the implementation of AML detection and investigation. In its 2004 and 2005 circulars (CBFA, 2004; CBFA, 2005), the regulator has specified the minimal criteria that should be met in developing an anti money laundering system.

1.1. Hypotheses: the anti money laundering complex and the compliance industry

This PhD research set itself the objective of gaining insight in the compliance function of financial institutions, based on the central hypothesis that the AML complex and the compliance industry are two parallel constructions, both working in the same domain, but on the basis of different objectives and motivations. These differences in motivation may not only result in differential attitudes and working methods, but also reveal the dilemmas that actors within AML are dealing with.

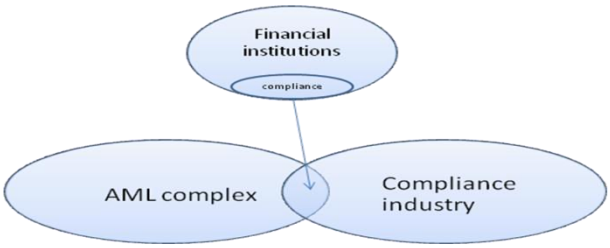

Figure 2 AML complex - compliance industry

The ***AML complex*** consists of the activities of private and public actors, carrying out regulatory, monitoring, reporting, investigatory and judicial tasks. The objectives of the AML complex are prevention, crime fighting and law enforcement, and it is based on legislation and regulation. As described by Buzan et al (1998), although the AML complex not linked to regions, but is a global system, it can be seen as a heterogeneous complex, consisting of a multiplicity of actors, surrounding, supporting or actively engaged in the battle against money laundering. The ***compliance industry***, on the other hand, is an entrepreneurial market providing services and tools in support of the fight against money laundering. This industry stimulates compliance and AML investments by providing monitoring systems, blacklists, training and advice to corporations that are obliged to implement the AML legislation. The compliance industry provides an additional service to AML regulation, in which AML compliance is marketed as a product for sale.

Financial institutions perform a pivotal role between these constructions, adding to and interacting with both the complex and the industry. The compliance officer, employed by the financial institutions reinforces this paradox. As go-betweens, they are continuously looking for a balance between the interests that derive from each structure: commercially oriented – within an entrepreneurial environment - or crime-fighting and -prevention. Based on this dual role, the complex and industry were studied from exactly this viewpoint.

2. Research questions

At the start of this research, we hypothesised that within the AML complex adverse attitudes are present, as different actors with dissimilar backgrounds are united. The outsourcing of government tasks to the private sector results in a paradoxical role for financial institutions. After all, the financial institutions' core business can clash with the monitoring task that is imposed by AML legislation; it is not always in a commercial interest to refuse customers or end client relationships. Looking into these potential contrasting interests can lead to an increased insight into the position of financial institutions and the norms they uphold, and to a view on the feasibility of imposing a surveillance function on private corporations. On the other hand, we also recognise interests that stimulate compliance within banks. Out of concern of risk management and foremost reputation protection, AML compliance can be encouraged. Regulatory sanctions also play a role in this respect, and serve as the stick in case of non-compliance.

The compliance officer bridges both worlds. In his/her role as inspector of employers, colleagues and clients, his function inherently implies a duality. The compliance officer is a new actor within AML; this function was only implemented in 2001, as a result of a regulatory obligation. The compliance officer is therefore a new and recent profession in Belgium that has some analogies with policing and private investigation. The compliance officer actually polices the money and determines the input of the AML chain, through their reporting duty to the FIU (Financial Intelligence Unit).

We derive the following research questions from the hypotheses:

1. *How does the AML complex function?*

Based on the compliance function within this complex, we try to map the operation, goals and perceptions of this complex. We will look for answers to the following questions: is there a cooperation or partnership between the elements of the complex? How does interaction take place? What are intrinsic motivations for each of the actors? To which extent is the current constellation feasible and what are the dilemmas and hindrances?

We have answered this first research question after phase 1 - 4 of this research, by making use of the results of a websurvey and interviews.

2. *What is the content of the compliance industry?*

A second research question is focused on the entrepreneurial market surrounding compliance: how is this compliance industry shaped en which services do we find? And secondly, what are reported reasons for its existence?

We have answered this research question after phase 2, 3 and 4, based on a series of interviews with both the compliance industry and the compliance officers.

3. *How can we fit in the compliance officer within these two constructions?*

This is the third and also the main research question. To which extent does the compliance officer actually find himself at the intersection or area of tension between commercial interests and rule-abidance? How is this function shaped and how do they carry out their investigations? Which interactions do we see between the complex, the industry and the compliance function? But also: what are explanations for the growth of this sector and to which extent is this a type of policing?

This core-question was answered after all four empirical phases of this research, combining the results of a websurvey and in-depth interviews with respondents from compliance departments, authorities and compliance industry. This resulted in gaining an insight in the separate construction and the position of the compliance officer, the leading actor in this research.

3. Methods and design

During this study use was made of a multi-methodological approach (Ponsaers and Pauwels, 2002; Bijleveld, 2005), implying a combination of quantitative and qualitative traditions. Both methods are complementary and may provide supplementary data. This decision was based on two grounds; first of all, we were moving in a research domain that had not been subject to criminological research in Belgium before, and we therefore had to take into account that a large investment was needed in order to make a first exploration of the sector. Secondly, literature had warned us against the access problems that may arise in studying the field of financial crime, in combination with private sector respondents (Geis, 1993; van de Bunt and Huisman, 2004).

This resulted in using a quantitative instrument, a websurvey, for the first phase of empirical data gathering, while relying on qualitative methods, semi-structured interviews, open source and literature research and observations, for the following phases. The websurvey allowed for reaching a larger amount of respondents at the same time, mapping their views and characteristics (Dillman and Bowker, 2001), and gave us the necessary basic information on which we could found the following phases. The subsequent interviews permitted a more in-depth dialogue with the respondents and could give more context to the earlier results[6].

3.1. Planning in phases

Every research consists of a technical research plan (Billiet, 2003). This study was divided in five phases, but we must note here that these phases were not as strictly defined as they may seem below. Actually the phases melted into one another – specifically the interviewing phases – which inevitably resulted in overlaps.

3.1.1. Literature study and document analysis (12 months)

This phase consisted of an exploration of the compliance domain and was carried out by means of studying literature on money laundering, compliance, corporate integrity, the legal framework on money laundering, self-regulation and government regulation in general, but also by studying open sources such as corporate governance charters of financial institutions, compliance codes and ethical codes. The official reports of the FIU were also studied in this period. As the compliance function had not been studied before, we had to invest rather much time in this exploration phase, and in the subsequent phases with regard to the entrance to the field.

3.1.2. Exploratory interviews with key informants and web survey (6 months)

In this second phase, we conducted exploratory interviews with a limited number of gatekeepers of the compliance field: compliance officers of the large banks in Belgium, the financial institutions' umbrella organisation and AML-consultants. Based on this information, combined with the information from the first phase, a websurvey (standardised questionnaire) was developed. As contact addresses of compliance officers were either not available or, if available, protected for reasons of privacy, we were not able to send the survey directly to the compliance officers. However, the umbrella organisation was willing to help us by sending the survey to all of their compliance

[6] More information regarding the methodology can be found in: Verhage, A. (2009a). Corporations as a blind spot in research: explanations for a criminological tunnel vision. *Governance of Security Research Papers Series I, Contemporary Issues in the Empirical Study of Crime*. M. Cools, De Kimpe, S., De Ruyver, B., Easton, M., Pauwels, L., Ponsaers, P., Vande Walle, G., Vander Beken, T., Vander Laenen, F., Vermeulen, G. Antwerpen, Maklu**:** 80-108.

contacts within the Belgian banks[7]. An e-mail was sent by them, containing an explication of the research and a link to the website where the survey could be filled out anonymously. A reminder was sent twice, in accordance with the Total Design Method (Dillman, 1991). This resulted in 74 filled out questionnaires, which were analysed by use of SPSS.

3.1.3. In-depth interviews with compliance officers and observations (12 months)

Subsequently and based on the results of the questionnaire, we contacted compliance officers of a diversity of banks. Contacts were made through telephone calls to general information telephone numbers, and via general e-mail addresses. In combination herewith, we also made use of the snowball method; after an interview, we asked respondents who they would recommend for an interview. This also helped identifying a number of respondents. The questionnaire had resulted in a general overview of the characteristics of the compliance sector, AML practices and viewpoints. During the interviews, we could go into some of these items more in-depth, checking our interpretation of the results, but also have a more profound understanding of a number of subjects. Some questions that were not answered in the questionnaire, could be answered through these interviews. In this phase maximum diversity was strived for, which implies that we contacted as well large and medium as smaller sized banks, in view of gaining insight in a broad array of compliance functions. In this phase, we interviewed 23 compliance officers, of whom 11 worked for large banks, 7 for medium-sized banks and 5 for small banks. The interviews lasted on average 1,5 to 2 hours. Most of the interviews were recorded on minidisc, unless the respondent refused recording, which was the case in two interviews. In order to be able to assess the contents of the interviews, and as a preparation for future interviews, most of them were typed out by the researcher herself. During this phase, additional observations of three AML-courses for bank employees took place. These courses were not only provided by the umbrella organisation but also by banks themselves. These provided us with support for our empirical results, as they allowed for a more informal contact with the respondents. The observations also resulted in a realistic view on the content and approach of AML within the bank, which allows for the mirroring of the interview results.

3.1.4. Interviews with members of the AML complex and the compliance industry (6 months)

Following the interviews with compliance officers, we also contacted other actors in the AML complex to gain an idea of their perspectives, practices in and opinions on anti-money laundering and compliance. In this phase, we interviewed respondents from the police services, both at a federal and an international level (6 respondents), the regulator and the FIU (3 respondents). Initially, we also intended to include judicial actors, but due to changes in personnel at the public prosecutor's office, the file analysis was postponed indefinitely. We tried to contact some lawyers to gain an insight in their views on the judicial phase of AML, but none of them responded. We did however succeed in involving members of the compliance industry in the interviewing phase. Six interviews were conducted with respondents from the compliance industry such as software-providers who develop AML monitoring tools, forensic accountants offering advisory services to banks or consultants.

3.1.5. Reporting, field-test-interviews and feedback to respondents (6 months)

Although some of the reporting was done in the course of this research, during the last six months the main reporting on the results of these interviewing phases was carried out. The interviews were analysed by means of Maxqda (Verbi, 2007), a software program for text analysis. By coding the

[7] The e-mail was sent by Febelfin to 208 persons; 2 compliance contacts per bank. In 2007, Belgium counted 104 banks. We do not know whether one or more respondents per bank filled out the survey. The response rate is therefore very difficult to calculate.

interviews, in total 41, we were able to bring some structure to the results. However, in order to limit the information (we had over 100 codes and almost 2000 coded segments), we divided the codes into clusters, allowing for a combination of coding results. These clusters were combined with the research questions and we reported accordingly. Secondly, we tested the results of our first reports. As the results of the first two phases were written down in articles, we decided to send these documents to some of our respondents, for a 'field-test'. Furthermore, the credit crisis crossed our study at the end of the interviewing phase and has in fact created a different banking landscape. This implies that some of the banks that were interviewed in 2007-2008 either have changed configuration or have dropped out of the picture altogether. In view of these radical changes in scenery, we returned to some of the banks in the spring of 2009 in order to grasp the impact of the credit crisis on the compliance function and the AML task. In combination with this test, we also carried out 3 more interviews in April and May 2009 with 2 compliance officers of large banks (both respondents were already interviewed in an earlier phase) and a member of the compliance industry.

3.2. Methodological conclusions

By combining both an exploratory, quantitative approach with an in-depth qualitative method, we were able to get both an overall and a specific view on the compliance sector, which allowed us to gather information on different levels. As we were dealing with an unknown sector, in a subject matter that has barely been studied in criminology, acquiring an overall view was indispensable at the start of this research. We would not have been able to ask the same questions during the interviews, without relying on the results of the questionnaire. Secondly, the results of the questionnaire gave us the opportunity to enter in a discussion with our respondents with regard to specific observations that we made during the analysis of the survey results. Furthermore, the interviews were crucial in providing a qualitative, in depth context for the survey results, and gaining insight in more 'sensitive' subjects, such as AML reporting and investigation. However, as always, we must be aware that the discourse that our respondents have applied, always implies a certain bias (Liedtka, 1992). Awareness of this bias also implies calculating in the fact that high-educated, professional respondents, within a professional setting, will not be inclined to completely speak their mind with regard to sensitive subjects of discussion. The use of a combination of research methods is one challenging way of tackling this bias (Crane, 1999). We actually did notice that results from the interviews were able to nuance or contextualise the survey results. A second manner to factor in 'social desirability bias', is by interviewing respondents from different services (public and private) that have different outlooks on the phenomenon, which allows for a cross-checking of the answers that are given, which we have done. Thirdly, we have looked for objective sources on the functioning of AML, such as judicial files, or FIU statistics. In both cases, we did not succeed in accessing this kind of information. With regard to judicial files, the public prosecutor's office had given us permission, but the analysis was postponed. With regard to FIU statistics, we could only make use of the statistics that are published in the annual report, as the FIU did not give us permission to analyse their own, more detailed data. This kind of information would have made a verification of the functioning of the AML complex and the reporting duty of financial institutions more profound.

After four years of research in this sector, we can state that the warnings in literature on the difficult access to the private sector, stimulating the use of secondary data, did not apply to the present study. Using secondary data turned out to be more difficult, due to access and practical problems, while the respondents themselves were, once found, rather open for research and willing to cooperate. Only one of the compliance officers that was contacted has refused to take part in this

research, due to lack of time. One of the banks even invited us to their in-house training on AML, and also the umbrella organisation has supported this research in the first phases.

From this we concluded that the timorousness of criminologists to study this sector seems unfounded and applaud other research in this field that could shed some light on effectiveness of the AML system. After this closer look at the methodology of this study, we now turn to the main empirical results.

4. Research results

4.1. Room for discretion in the AML system

The fight against money laundering in Belgium (and abroad) is based on a *risk-based approach (FATF, 2007)*. Instead of focusing on mere rule-abidance or the application of objective indicators, a system was installed that provided room for interpretation and discretion. The focus of this system is on the investigation of transactions and clients that represent a higher *risk* of money laundering. The system is based on 'intelligent reporting' (as opposed to automatic reporting on the basis of specific objective criteria): banks are therefore allowed room for discretion with regard to reporting transactions to the FIU. Intelligent reporting also implies that the bank functions as a first filter before cases are transmitted to the FIU, potentially resulting in a more efficient functioning of the system. On the other hand, this discretion also implies that the position of the compliance officers is inherently linked to many dilemmas.

On top of that, since the implementation of the AML legislation in Belgium and more specifically since the regulator has obligated the instalment of the compliance function (CBFA, 2001a), money laundering (and probably to a larger extent any association with the financing of terrorism) has become a liability and a risk for banks (Zimiles, 2004). De sanctions that were imposed on a bank such as ABN-Amro in 2005[8] illustrate this. The consequences of this sanction were specifically large with regard to the repair policies that this bank had to implement in view of her compliance policy: hiring external advisors, implementing new procedures and compliance programmes, but also the hiring of 300 new compliance staff members (ABN Amro, 2005). This and other cases have shown that it is of crucial importance for banks to protect themselves from this risk. The compliance officer fulfils a central and essential task in this respect.

4.2. The compliance officer

The compliance officer, as we stated earlier, the central person responsible for the implementation of anti money laundering tasks (next to a number of other tasks related to 'the integrity of banking' such as prevention of insider trading, checks on privacy regulation, checks on new advertises, and so on - CBFA 2001a), takes up a very specific place in the battle against money laundering. In the survey that was sent to the compliance officers in the first, exploratory phase of this study, we asked for a number of general characteristics of compliance officers. Their answers showed that Belgian

[8] ABN-Amro was imposed a sanction in 2005 by the US regulator for a total of 80 million dollars as a fine for neglecting anti money laundering procedures, lack of thorough monitoring and non-reporting of specific transactions with Iran and Libya. The bank was also obliged to elaborate a more thorough compliance programme. (Simpson, G., How Top Dutch Bank Plunged Into World of Shadowy Money. *Wall Street Journal,* 30/12/2005)

compliance officers are often male (although there are a few female compliance officers), economists or lawyers, and often have developed their career within the bank (Verhage, 2011). As such, they can rely on years of experience within the bank, together with a thorough knowledge of its functioning.
In contrast with their compliance colleagues in other European countries (such as for example France), Belgian compliance officers in general do *not* have a law enforcement background (such as a career in the police). This is surprising, as in France we see the opposite: compliance officers often do have a police background and are hired by the bank because of it (Favarel-Garrigues, Godefroy et al., 2008). Their police backgrounds do not only imply that they have gained experience in the investigation of all that is suspicious, it also results in very smooth contacts between the police services on the one hand and compliance departments in France on the other hand, based on their old boy's network. Information exchange is therefore rather easy and informal, while in Belgium these relations seem to be more formalized which makes public actors less accessible. In France, this is even seen as an important condition to carry out compliance tasks successfully (Favarel-Garrigues, Godefroy et al., 2006).

Considering the difficult position of the compliance officer within the bank (having to make decision that might go against the commercial interests of the bank), independence of this function is crucial. The regulator has tried to build in this independence by giving compliance officers a number of basic rules, which should enable them to carry out their tasks independently and objectively. Because of their complex function and responsibility, compliance officers should have direct access to the highest management function (Thierens, 2004). The Basel guidelines[9] also specify that the compliance department should be allowed a specific statute within the banking organization and should be protected by a compliance charter (BCBS, 2005). This charter should be approved by the management and should (among others) contain which lines of responsibility exist, which incompatibilities there are and stipulate that compliance tasks cannot be outsourced (Thierens, 2004).

In spite of these guarantees, the compliance officer remains a bank employee, and hence a part of a commercially oriented organisation. This might entail a number of role conflicts (especially in those – small number of – cases where a compliance officer is asked to combine both a commercial and a compliance function). The survey showed that the compliance officer indeed often feels positioned between the hammer and the anvil; on the one hand he is an employee, part of a commercial environment, but on the other hand he is responsible for the implementation of legislation that might violate commercial interests as it may lead to the elimination of client relationships, the blocking of specific transactions or the renunciation of a client relationship at the start.

Compliance officers have indicated in the survey that they have several objectives at heart in their jobs. These objectives vary from general goals such as 'crime fighting' to 'preserving the integrity of the financial system', but also 'protecting the bank's reputation' (Verhage, 2009a).

The discretion that is inherent to the *risk-based approach* on money laundering was considered, both in the survey and in the interviews with compliance officers, as something positive as it leaves room

[9] Basel Committee for Banking Regulators, consisting of representatives of central banks and regulators (www.bis.org/bcbs/).

for discretion and makes banks think for themselves. It also allows for a thorough insight in the banks clientele and their activities. It however also carries with it a number of insecurities. The compliance officer is now left alone in his decision on what is suspicious, a-typical or deviant, which 'suspicious' transactions should be investigated, which of them should be reported and, finally, what this should imply for the client relationship once an investigation has been carried out. This implies that responsibility for these decisions is placed with the bank. When the compliance officer is not equipped to make this kind of decision or, at least, advise on this, this becomes a very difficult balancing act. Basic information, respondents stated, now is often lacking, or at least not provided by the regulator or the FIU. Apart from this, a number of basic procedure have been developed by the regulator, that should form the basis for a system of thorough transaction monitoring. These procedures and the dilemmas that go along with them, are discussed in the following paragraphs.

4.3. Suspicious transactions

4.3.1. Detection and prevention

Apart from the obligation to develop a compliance function in each bank, the regulator also introduced a number of requirements in the battle against money laundering (CBFA, 2005). These requirements entail for example the know-your-customer duty (mapping the background and economic activities of the client), client acceptance policy (risk assessment), client identification duty (checking blacklists) and the instalment of a **first and a second line** of detection concerning money laundering transactions. This latter requirement implies that two types of procedures for the detection of suspicious transactions should be implemented. Both 'lines' are based on the risk-based approach: the detection of specifically those transactions and clients that might be a risk for the bank (FATF, 2007). Each bank needs to build its own policy and procedures, founded on the risks that they have identified, the profile of the banks and its clients, and his/her activities.

The *first* line of detection is based on the awareness and vigilance of employees (CBFA, 2005). Banks are expected to train their employees in anti money laundering and help them recognize atypical transactions, or money laundering schemes and constructions. It goes without saying that training and attentiveness are crucial in this regard. Banks are also supposed to provide their employees with criteria that should help them detecting suspicious transactions and clients, which should allow them to report those cases to the compliance department. The compliance department is required to start an investigation after the report of the first line has reached them. However, our research has suggested that the first line of detection often remains limited to stereotypical money laundering cases ("the nervous man with a large suitcase of money that enters the bank" - (Verhage, 2009a)), even though the large majority of banks have introduced structural training for their employees. Employees working at the desk of a bank (as it is them who are functioning as first-line detectors), are often very busy and short on time and expertise to detect complex money laundering schemes. They do, however, have the advantage of 'local knowledge': they often have access to grey information: stories about the different types of "businesses" in which their clients are involved. After all, rumours can also be a valuable source of information with regard to detecting money laundering patterns.

The *second* line of detection no longer depends on the personal alertness of individuals, but introduces an automated monitoring: the monitoring system. The circular specifies that banks need to implement 'a control system that detects atypical transactions' of all accounts and clients. In the circular, it is stated that banks, that can demonstrate that they do not need an automated system of monitoring because of the amount or volume of their transactions, are allowed to carry out this

monitoring task manually (CBFA, 2005).It may be clear that not many Belgian banks will be able to demonstrate that they can manually check all accounts and transactions of all clients in a reliable way (banks process thousands of transactions on a daily basis). Therefore, the majority will resort to monitoring software, allowing them to monitor all transaction on a daily basis, based on pre-set criteria and typologies. This second line of monitoring is supposed to enable the compliance department to systematically detect transactions that, although not recognized as such by the first line, can be characterized as atypical or even suspicious.

In practice, this implies that in the majority of banks, a monitoring system is put in place, often provided by a large software provider, that is founded on a set of if-then scenarios and comparisons of client-behaviour between today and the past. Monitoring software looks at the profile of the client, its past and current transactions (the monthly income, weekly expenses, etc.) and compares that to the transaction that is taking place (KPMG, 2007; Verhage, 2011). Some software packages provide about a 100 'out of the box' scenarios that are ready to go once they are installed, according to one of our respondents. Furthermore, it will take into account transactions to or from countries 'at risk' (such as currently Iran and Korea – CTIF-CFI, 2010) or transactions towards or by "politically exposed persons". Politically exposed persons are persons who – as a result of their political position - can pose a risk in terms of money laundering or terrorism financing[10]. This does not have to imply automatically that these PEP's are a risk per se. It does however, mean that increased inspection of their transactions is needed (Pieth and Aiolfi, 2005). Banks also pay high attention to these PEPs (KPMG, 2007) and Belgium was for a long time considered to adopt a very broad approach to these PEPs (even including Belgian citizens) (IMF, 2006). Today, in Belgium the scope is more limited as a result of a single focus on the foreign PEPs (Deloitte, 2011). The criteria are updated regularly, depending on international evolutions. For example currently, also politicians from Egypt and Tunesia (CTIF-CFI, 2011) fall within this category.

As a result of these controls and checks, 'alerts' arise that, according to our respondents, may vary from 20 – over 100 a day. In practice, a compliance department will try to fine-tune their systems to that extent that a 'manageable' number of alerts is the result (Verhage, 2011). Of course, how they 'set the systems' will determine the usefulness of these systems and the extent of preventive power. The emphasis on risk-based analysis also results in a very high workload in view of proactive policing by the compliance officers. From a human rights perspective, these controls and checks also imply that this permanent surveillance of customers and colleagues is relatively intrusive, leading one of the compliance officers to say "*This is a true Stasi-situation*" (Verhage, 2011).

4.3.2. Investigation

After the detection of a number of potentially suspicious transactions, the compliance officer is supposed to investigate these more in-depth. Compliance officers are forced to prioritise: not every alert can be investigated. Moreover, many alerts are false alarms (one of our respondents stated that 99% of all alerts are 'false positives'– Verhage, 2011).

The investigation of alerts is carried out making use of a diversity of sources. Compliance officers do not have formal sources (such as criminal convictions) at their disposal and therefore have to make use of information that is publically accessible. This implies intensive use of information that is already present within the bank (on the client, his/her family, and his/her financial activities). Furthermore, compliance officers also find a lot of information in open sources: the Internet, use of

[10] The Directive Art. 3 (8) refers to PEPs as follows: 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.

trade databases, and so on. In some cases the local banking office is contacted to gather more background information on the client. Compliance officers of other banks can also supply useful information (for example whether someone is also under investigation by their department)[11].
A minority of the respondents also stated that they incidentally contacted police officers or the FIU to gather off-the-record information. This type of information cannot be written down in the formal file and will not be transmitted to the FIU when the files is reported. In most cases the available information is sufficient to be able to assess the case. The analysis of the transaction and the client is also checked with its risk level, the sector in which he/she is active, the countries involved, the amount of money involved, and so on. For this assessment the FIU and other typologies are used intensively. What is seen as 'suspicious' however remains an individual interpretation and a subjective decision.

4.3.3. Reporting

Compliance officers decide, according to the policy of the bank, to report (or not report) (a selection of) suspicious transactions to the FIU. To give an idea of the volumes: in 2010 banks made 3870 reports to the FIU in Belgium (the number of reports varies between 4.400 and 3.600 the last 5 years). More than half of all Belgian banks has made a report (58/105 banks) and over 60% of all reports to the public prosecutor by the FIU was based on reports by banks (CTIF-CFI, 2011).
Banks, as stated, have limited access to formal information to base their judgment on, to be able to assess whether the transaction concerns a 'true' suspicious transaction or not. This results in the fact that banks have to decide whether or not to report a client based on incomplete information (with possible negative commercial consequences), or that they decide to follow the client until they have more certainty about their activities. The interviews showed that banks – as a consequence of this uncertainty - have developed a reporting strategy, based on the earlier mentioned criteria on 'atypical' or suspicious, but also based on an assessment of the risk a bank runs in case of non-reporting. The current application of the anti money laundering legislation carries the danger in it that banks will report defensively, to prevent sanctions by the regulator and potential reputational damage. The FIU also advises to report 'when in doubt'. But 'unfounded' reporting a client can also have negative consequences. The respondents referred to cases in which complaints were made by clients against banks after a money laundering report to the FIU, or a case in which staff was threatened because of a report. These kind of situations may lead to a hesitation to report again. Respondents in this respect also referred to the fact that during investigations and interviews, police services sometimes mentioned the name of the bank that had made the report. This is of course detrimental for any relationship between banks and FIU, as this needs to be based on trust.

4.3.4. Consequences for the client ?

A report to the FIU does not necessarily imply that the client relationship will be terminated, nor does it mean that it will have no effect. This decision varies per bank and is a case by case decision. It depends on the type of client involved, the number of evidence, the policy of the bank, the volume of money involved, and so on. Some banks state that they have a policy that any association with

[11] This has become an allowed practice after the implementation of the 3rd Directive in 2010 (European Parliament and the Council of Europe (2005). *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*.)

suspicious money or clients should be avoided, and will therefore end the client relationship, other banks state that they on the contrary want to follow the client further. To prevent problems, some banks have excluded 'cash-clients' from their clientele (night shops, second hand car dealers, etc.). The fact that banks, as our respondents state, get no feedback whatsoever from the FIU on their report (apart from information on files that have been dismissed), also implies that this decision is left entirely to the bank.

4.4. The functioning of the AML complex

Apart from the activities of compliance officers and their attempts to shape the anti money laundering policy of banks, the research also aimed to get a view on the broader picture of the battle against money laundering through the money laundering chain. The visions of several actors within this chain were therefore mapped, looking for views on the current practice of anti money laundering, but also on how other actors function within the complex. We will discuss the most important results.

One of the most remarkable and recurrent findings of this study was the lack of feedback within the anti money laundering chain. Information provision mainly goes one way: from banks to the law enforcers. Also in this direction, however, information provision is limited to what banks want the law enforcers to know, and what they are obliged to report in view of the reporting duty. The mutual sharing of information is rather limited, and there is very little will to change this. This lack of information sharing and transparency – with regard to providing feedback, but also about non-reported atypical constructions – may not have a very positive effect on the functioning of the system. On top of that, the anti money laundering complex does not build the knowledge that it might build in theory; knowledge accumulation is very restricted. This results in the fact that banks need to fall back on the annual reports of the FIU or on information that is provided by commercial organisations. The danger of this is that the same analyses are confirmed over and over again and that the focus is on stereotypes of money laundering (the usual suspects such as cash-carriers, second hand car dealers or drug dealers) and discovers very few new, more complex constructions, or, worse, focuses on the wrong kind of cases.

Cooperation between public and private actors in the chain cannot be seen as smooth. Opposed to their French colleagues, Belgian compliance officers cannot fall back on their former colleagues in law enforcement, which might explain the lack of cooperation partially (Favarel-Garrigues, Godefroy et al., 2008). A minority of our respondents stated that they exchange some information on an informal basis, but this is mainly based on personal contacts or years of cooperation. Although police respondents state that most of the banks make considerable efforts in anti money laundering, compliance officers perceive their position in the chain differently; they state that they are seen more as suspects or accomplices than as partners in crime control. The investigation and reporting of transaction is bound to be influenced by this perception.

Among banks we see a high level of informal cooperation. Compliance officers know each other (it is a small world) and are now also allowed to exchange information on investigations. More formal possibilities for cooperation and information exchange is applauded by the respondents. It would

allow for a combination of information by different banks (knowledge-accumulation), which should enable banks to recognise clients in an earlier stage and see clusters of clients and transactions. Secondly they plead for the development of a blacklist of clients, which could prevent bank shopping by clients – clients who will look for the least strict bank will be discovered soon. Our police respondents further stated that they lack insight in the monitoring systems and the criteria that are used within banks. The tools that are used by banks may very well provide the police with useful information, for example relating to criteria, scenarios or volumes of transactions, but information exchange on this issue is very limited. Police services are not informed on the way in which these mechanisms are applied, whether checks are run manually or by use of software, etc. On the other hand, compliance officers stated that they would be very interested in learning which patterns are detected by police services, in order to enhance their monitoring systems. Of course, we here have to point at the necessary guarantees that should be built in for this exchange of information, both with regard to interbank communication and between public and private actors.

Another consequence of the cooperation between banks is the installment of an informal type of social control with regard to the level of compliance. Compliance officers told us that the sector indeed knows which banks stick to the rules and which do not. Banks will take this into account in their business relations with these banks, or by making this known within the sector. This implies the development of an informal sanction mechanism, also based on the risk that these non-compliant banks may pose for other banks.

5. The compliance industry as a vehicle for investments

A final part of this study aimed to discuss the place of the compliance industry in the battle against money laundering. The compliance industry comprises the whole range of services, instruments, information sources, trainings and so on that might support organisations in the battle against money laundering.

Banks have a number of motives to make use of the compliance industry. First of all, they are subject to the legal obligation to monitor transactions and clients (the second line of control, as we discussed earlier (CBFA, 2005)). This monitoring is in most cases automated, implying that banks are obligated to appeal to one of the corporations within the compliance industry. These companies sell software that enables this type of monitoring or name-matching. The usefulness of these systems may be questioned; In our research, the use of this type of second-line monitoring was questioned by both the compliance industry and a number of compliance officers. In their view, the added value of software can be doubted. After all, the quality of detection methods of these software systems, depends largely on what has been put into the system. The quality of the scenarios, the reliability of the data that makes part of the system and how it is fine-tuned all determine the output of the system and the number of false alerts.

When we combine this legal obligation with the fact that anti money laundering legislation remains rather vague on the criteria that might lead to an atypical or suspicious transactions, and that further information provision on this is very limited, we may conclude that banks might be inclined to make use of external experts in anti money laundering such as forensic auditors (e.g. the “Big Four”,

compliance advisors or software providers to gather more information. This is not only often done to make sure that banks are well informed and prepared for their task of anti money laundering, but also to protect the banks' reputation and its competitive position towards other banks by preventing sanctions by the regulator. This however also implies that current regulation and legislation stimulates the existence of a commercial market on compliance and AML. As such, we may conclude that the anti money laundering complex and the compliance industry are mutually reinforcing constructions. The compliance industry capitalizes on this by reinforcing the threat of money laundering and dramatizing its risks (Ericson and Haggerty, 2002).

We could derive from the interviews that banks are looking for the golden mean in investments in compliance; the *benchmark* for investments in compliance and AML investments that is used in this sense is then to a large degree prescribed by other banks. Banks do not want to be on the front row when it comes to compliance investments, but not at the bottom either. This benchmark is however also laid down by the activities and supply of the compliance industry and the extent to which the regulator exercises control and supervision on AML. After all, potential liability can be a "*strong incentive for banks to tighten their compliance procedures"* (Smith and Cooper, 2009)
An important question that arises here is whether we want to leave this kind of information provision to a commercial market that in the end profits from the stimulation of anti money laundering activities. The provision of blacklists of clients' names, as now carried out by commercial organisations, is after all a very sensitive activity. We will get back to this later.

6. Effects and side effects of the anti money laundering complex

6.1. A limited view on effects of the AML chain

In conclusion to the discussion of the research results, we aim to give a short outlook on the effects of the system as known today. Evaluating the AML system is very difficult as we lack measurable results (after all, what does the system prevent?). There is no benchmark to start from and today we have no clear system to measure the volume of black money, let alone the amount of money that is laundered. A number of figures are stated (Schneider for example calculated that the underground economy in Belgium amounts to 18,3% of the official GDP; Schneider, 2011), but these figures remain estimates (van Duyne, 2006).

A second-best solution therefore is to have a look at the results on the level of the penal chain. We have done this by looking at the figures that are stated by the FIU in her annual report. We need to remark here that there are measurement problems on every level of the AML chain. The results of the figures by the FIU show that for the period 1993-2006, about 11% of all files that reach the public prosecutor's office, results in a conviction. This is 3,7% of all FIU files from 1993 until 2006. The results on the level of law enforcement seem rather limited after 13 years of AML. Of course we need to take into account that the compliance function within banks was only introduced in 2001. We cannot derive from the statistics that are available to which extent the reports by banks have resulted in convictions. We desperately need better statistics to be able to make an evaluation (Verhage, 2010). However, we do know that the same limited results are found in other countries when the same type of evaluations are attempted (Levi, 1997; van Duyne and de Miranda, 1999).

6.2. Side effects

Some authors refer to the displacement effect that might occur when certain types of money laundering instruments are controlled more strictly (van de Bunt for example refers to Hawala banking in this respect (van de Bunt, 2008)). We will not discuss this any further in this contribution. There are, however, other side effects of the implementation of the anti money laundering system. A more intrusive dilemma refers to the fundamental questions that arise when looking at the battle against money laundering, especially since this has been accompanied by the fight against terrorism financing since 2001. Fundamental rights such as privacy and due process may be at stake. Furthermore, we may ask ourselves – as the fight against money laundering is inescapably risk oriented, making use of scenarios and risk profiles – to which extent certain categories will be focused on and targeted simply because they fit the profile, even though they may not pose any threat[12]. After all, criteria are by definition used to exclude certain groups and include others.

Rights of defense are interpreted relatively narrow in this system. Whereas in a proactive police investigation there needs to be a 'reasonable suspicion of (future) criminal activities' (Vanderborght, 1999), this threshold does not apply in AML for banks. They are even expected to investigate in case of minor suspicions. In this respect, democratic controls on this process should be optimal.

7. Conclusions

A first conclusion of this study is that compliance and anti money laundering seem to have permeated the Belgian banks in general. When we look at the level of the banks themselves, we see that from time to time a compliance officer has to fight his battles, balancing between commercial interests and rule abidance. This is probably inherent to the anti money laundering task and does not conflict with the conviction that without compliance banks can no longer function.

A second conclusion relates to the results of the battle against money laundering: a new form of policing has emerged, described by many. Sometimes this is referred to as 'new policing' (Levi, 1997), banking detectives (Kochan, 2006) the transnationalisation of policing (Sheptycki, 2000) or "policing the money". This implies that the compliance officer has become one of the new actors in the policing landscape and adds to the *multilateralisation of policing* (Favarel-Garrigues, Godefroy et al., 2008). The introduction of the term AML complex is therefore useful as it makes clear that a multitude of actors, from different backgrounds and with a diversity of motives, is active in this field. It also illustrates the differences in power positions of each actor involved in this battle.

Furthermore, we conclude that responsibility in the AML complex is placed at the base of the complex: with reporting institutions. The question remains how this system aims to prevent and fight crime when this base is not provided with sufficient information. This after all urges banks to make use of (outdated) stereotype criteria on the one hand, or to develop criteria by themselves on the

[12] For example the Flemish women P. Vinck and her husband N. Sayadi have been on blacklists since 2003 based on suspicions of links with terrorist groups. There was no official evidence for this. These types of blakclists were criticised earlier, also on the level of the Council of Europe (De Morgen, 2007). It took years for their names to be removed from the official United Nations list on the basis of a Regulation by the European Commission (in July 2009) (Nr. 678/2009).

other hand, resulting in the fact that the banks determine the threshold for reporting and are forced to make use of the services of the compliance industry. When the compliance industry is responsible for determining these criteria and providing information such as blacklists, we undoubtedly encourage the application of quality standards for their services and instruments, provided by the authorities. The quality of monitoring systems today is stated to be very different, and may lead to a false feeling of security.

Finally we conclude that the non-transparency of norms and concepts surrounding 'risk' that are used throughout the battle against money laundering can have an important impact on fundamental rights. We have posed the question to which extent the costs this system are in proportion with the benefits. As the AML system is currently characterised by a reactive approach, based on information from the past (Crawford, 2009), that is also limited in scope and sources (Gelemerova, 2009),the danger exists that this is a static system that is preserved and predestined to find the same usual suspects again and again.

References

ABN Amro (2005).
http://www.group.abnamro.com/pressroom/pressreleasedetail.cfm?ReleaseID=278325.

BCBS (2005). *Compliance and the compliance function in banks***:** 16.

Bijleveld, C. (2005). *Methoden en Technieken van Onderzoek in de Criminologie*. Den Haag, Boom Juridische Uitgevers.

Billiet, J., Waege, H., (2003). *Een samenleving onderzocht. Methoden van sociaal-wetenschappelijk onderzoek*. Antwerpen, De Boeck.

Buzan, B., Wæver, O, De Wilde, J. (1998), *Security: A New Framework For Analysis*. London, Lynne Rienner Publishers.

CBFA (2001a). *Circulaire D1 2001/13 aan de kredietinstellingen*.

CBFA (2001b). *Bijlage aan de circulaire D1 2001/13 van 18 december 2001 over 'compliance'*. CBFA.

CBFA (2004). *Reglement van 27 juli 2004 van de Commissie voor het Bank-, Financie- en Assurantiewezen betreffende de voorkoming van het witwassen van geld en de financiering van terrorisme (regulation of 27 July 2004 of the CBFA regarding the prevention of money laundering and terrorist financing) B.S.* 22.11.2004.

CBFA (2005). *Gecoördineerde versie d.d. 12 juli 2005 van de circulaire van de Commissie voor het Bank-, Financie- en Assurantiewezen over de waakzaamheidsverplichtingen met betrekking tot de cliënteel en de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme*.

Crane, A. (1999). "Are You Ethical? Please Tick Yes □ Or No □ On Researching Ethics in Business Organizations." *Journal of Business Ethics* **20**(3): 237-248.

Crawford, A., (2009) "Governing perceptions of crime and (in)security in an age of uncertainty", paper for the Final Crimprev Conference 'Deviance, Crime and Prevention in a Punitive Age', June 2009.

CTIF-CFI (2011). *Jaarverslag 2010*.

De Morgen (2007). *Zwarte lijsten terroristen schending mensenrechten (Blacklists terrorists violate human rights).* 11/11/2007.

Deloitte (2011). *Final Study on the Application of the Anti-Money Laundering Directive*. European

Commission**:** 347.

De Morgen (2007). *Zwarte lijsten terroristen schending mensenrechten (Blacklists terrorists violate human rights).* 11/11/2007

Dillman, D. and D. Bowker (2001). The Web Questionnaire Challenge to Survey Methodologists. *Dimensions of Internet Science*. U. Reips and M. Bosnjak. Lengerich, Pabst Science Publishers.

Dillman, D. A. (1991). "The Design and Administration of Mail Surveys." *Annual Review of Sociology* **17**(1): 225-249.

Ericson, R. and K. Haggerty (2002). *Policing the risk society*. Oxford, Clarendon Press.

European Parliament and the Council of Europe (2005). *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*.

FATF (2007). *Guidance on the Risk-based appraoch to combating money laundering and terrorist financing. High level principles and procedures*.

Favarel-Garrigues, G., T. Godefroy, et al. (2006). *Les banques, sentinelles de l'anti-blanchiment. L'invention d'une spécialité professionelle dans le secteur financier*. Paris, CERI**:** 248.

Favarel-Garrigues, G., T. Godefroy, et al. (2008). "Sentinels in the Banking Industry. Private Actors and the Fight against Money Laundering in France." *British Journal of Criminology* **48**: 1 - 19.

Geis, G. (1993). The Evolution of the Study of Corporate Crime. *Understanding Corporate Criminality*. M. Blankenship. New York, Garland**:** 3-28.

Gelemerova, L. (2009). "On the frontline against money-laundering: the regulatory minefield." *Crime, Law and Social Change* **52**(1): 33-55.

IMF (2006). *Belgium: Report on the Observance of Standards and Codes. FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism*, IMF Country Report No. 06/72**:** 17.

Kochan, N. (2006). *The Washing Machine. Money, Crime and Terror in the Offshore System.* London, Duckworth.

KPMG (2007). *Global Anti Money Laundering Survey 2007. How banks are facing up to the challenge*.

Levi, M. (1997). "Evaluating the 'New Policing': Attacking the money trail of organized crime." *The Australian and New Zealand Journal of Criminology* **30**: 1-25.

Levi, M. (2002). "Money Laundering and its Regulation." *The Annals of the American Academy of Political and Social Science* **582**(1): 181-194.

Liedtka, J. M. (1992). "Exploring ethical issues using personal interviews." *Business Ethics Quarterly* **2**(2): 161-181.

Naylor, R. (2007). *Criminal profits, terror dollars and nonsense*. Tax Justice NL, Seminar on Money Laundering, Tax Evasion and Financial Regulation Transnational Institute Amsterdam.

Pieth, M. and G. Aiolfi (2005). *Anti-Money Laundering. Levelling the Playing Field*. Basel, Basel Institute on Governance**:** 48.

Ponsaers, P. and L. Pauwels (2002). De methodestrijd in de criminologie. *Criminologie in Actie. Handboek criminologisch onderzoek*. K. Beyens, J. Goethals, P. Ponsaers and G. Vervaeke. Brussel, Politeia**:** 55-72.

Schneider, F. (2011). *The shadow economy and shadow economy labor force: what do we (not) know?* Discussion paper N°5769, Discussion paper series IZA (Institute for the Study of Labor), Bonn, 66p.

Sheptycki, J., Ed. (2000). *Issues in Transnational Policing*. London, Routledge.

Smith, J. D., Cooper, G., (2009). "Disrupting Terrorist Financing With Civil Litigation." *Case Western Reserve Journal of International Law* 41(1): 65-84.

Thierens, F. (2004). "De compliance functie in België." *Tijdschrift voor Financieel Recht*(3): 778-794.

van de Bunt, H. (2008). The Role of Hawala Bankers in the Transfer of Proceeds from Organised Crime. *Organized Crime: Culture, Markets and Policies***:** 113-126.

van de Bunt, H. and W. Huisman (2004). "Organisatiecriminaliteit." *Tijdschrift voor Criminologie* **2**(46): 106-120.

van Duyne, P. (2006). "Witwasonderzoek, luchtspiegelingen en de menselijke maat " *Justitiële Verkenningen* **32**(2): 34-40.

van Duyne, P. and H. de Miranda (1999). "The emperor's clothes of disclosure: Hot money and suspect disclosures." *Crime, Law and Social Change* **31**(3): 245-271.

Vanderborght, J. (1999). "Het doel heiligt de middelen? Proactieve recherche in de strijd tegen georganiseerde criminaliteit. ." *Custodes* **1**: 13-32.

Verhage, A. (2009). "Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry." *Crime, Law and Social Change* **52**(1): 9-32.

Verhage, A. (2010). The holy grail of money laundering statistics: Input and outcome of the Belgian AML system. *Cross-border crime inroads on integrity in Europe*. P. van Duyne, Antonopolous, G., Harvey, J., Maljevic, A., Vander Beken, T., Von Lampe, K., . Nijmegen, Wolf Legal Publishers**:** 143-168.

Verhage, A. (2011). *The Anti Money Laundering Complex and the Compliance Industry*. London, Routledge.

Zimiles, E. (2004). "KPMG Survey: Banks accept more costly Money Laundering Laws, Expect heightened cooperation with regulators." *The Journal of Investment Compliance*: 26-30.