Money Laundering
and Money Laundering Countermeasures:

International Regime versus Technological System

Heidi Bøkestad Utvik
University of Oslo
“Globalisation, Innovation and Policy”
2004

Word count: 23 151
“Money Laundering and Money Laundering Countermeasures: International Regime versus Technological System”

ESST
The European Inter-University Association on Society, Science and Technology
http://www.esst.uio.no

The ESST MA

Heidi Bøkestad Utvik
hutvik@hotmail.com
First and second semester university:
University of Oslo
Second semester specialization:
“Globalisation, innovation and policy”
Supervisor: post doc. Bent Sofus Tranøy
Word Count: 23 151
Synopsis

Money laundering has increased in scope and is believed to contribute to disruption of the financial system and uphold drug trade, trafficking of women and children for commercial sex, weapon smuggling, and terrorist financing. It is not only conducted by traditional criminals, but is often assisted by corrupt financial institution officials. The expansion of finance capitalism allowed for worldwide capital flows in a weakly regulated financial system. Financial havens and electronic payment technologies supporting anonymous customer relations have in turn offered opportunities to launder illicit proceeds without raising suspicion from public authorities.

In the late 1980s an international anti money laundering (AML) offensive was initiated. Under direction of the Financial Action Task Force (FATF), international standards have been developed and adopted within many countries’ national policy frameworks. The terrorist attacks of September 11th 2001 gave rise to a policy u-turn in international AML. Whereas collaboration before this incident centred on tracing criminal money after crime commitment, post-September 11th 2001 collaboration took on a preventive risk-based approach seeking to predict possible terrorist attacks.

This thesis examines money laundering and AML techniques, drawing on ideas from the science, technology and society (STS) tradition. It explains the driving forces behind enhanced international action against the problem and demonstrates that an international AML regime has emerged. The regime possesses the features of a technological system, and this influences AML policies. The analytical framework combines three approaches of regime theory with Thomas P. Hughes’ theory of technological systems.

The various approaches are both competing and complementing and prevail at different stages of the regime process. Regime formation is explained by US hegemony, suitable with the power based approach. Regime maintenance centres around the work of the FATF and is rooted in the recognition that fighting money laundering in a collaborative manner is more beneficial than negotiating several bilateral agreements, which is consistent with the interest based approach. International AML is influenced by expert knowledge. This expert knowledge can be explained both by epistemic communities exemplary of knowledge based theories, and by technical authority exemplary of the technological systems approach.

Keywords: money laundering - electronic payment technologies - cyberpayments - financial havens - secrecy - transparency - AML - FATF - international regime technological system
Preface

“Scholars of international political economy have been slow to show interest in the study of illicit activity in global finance. Particularly neglected has been a focus on the response of states to the growth of this activity” – Eric Helleiner, 1999

This thesis investigates the response of countries to money laundering. Having been interested in the topic for quite a while, I was happy to realize that it could be a relevant subject for my Master Dissertation.

In October 2003 my sister called to tell me that judge Eva Joly was going to give a lecture about financial crimes at the Oslo University College Faculty of Journalism and Information Science. With a borrowed admittance card I snuck in and attended the lecture. It left me with great inspiration to dive into the subject and investigate it further. When I was given a go-ahead tone that this could be an appropriate topic for an ESST Master Dissertation from the coordinator of my second semester specialization, the wheels started spinning.

The journey from thesis outline to final product has been challenging and I indeed enjoyed the ride. I would like to thank the following people for their support, help and inspiration:

the SAS Institute AS who allowed me to attend their money laundering seminar early in May, where I came into contact with several of my interviewees; the people who kindly took time from their working hours to be interviewed; my supervisor post.doc. Bent Sofus Tranøy for keeping me on a leash and without whose advice and insight I probably would be very lost; my boyfriend for proofreading and much needed support and encouragement when things looked the worst; my father-in-law for proofreading and useful comments; my sister for indirectly giving me the idea of my master topic; my fellow first and second semester ESST students for a good time during a good year both socially and professionally, and in particular Anne-Grethe Sandvik for good advice and moral support.
# Table of contents

SYNOPSIS
PREFACE

## 1 INTRODUCTION

1.1 MONEY LAUNDERING - THE SCOPE OF THE PROBLEM
1.2 MONEY LAUNDERING COUNTERMEASURES - THE SCOPE OF RESPONSE TO THE PROBLEM
1.3 MOTIVATION: MONEY LAUNDERING IN CONTEXT
1.4 OBJECTIVES AND RESEARCH QUESTION
1.5 METHODOLOGY
1.6 THESIS STRUCTURE

## 2 COLLABORATION: INTERNATIONAL REGIMES VERSUS TECHNOLOGICAL SYSTEMS

2.1 DEFINING AN INTERNATIONAL REGIME
2.2 THREE SCHOOLS OF REGIME THEORY
2.2.1 POWER BASED THEORIES
2.2.2 INTEREST BASED THEORIES
2.2.3 KNOWLEDGE BASED THEORIES
2.3 TECHNOLOGICAL SYSTEMS
2.4 SUMMARY OF EXPECTED FINDINGS

## 3 FACILITATING AND FIGHTING MONEY LAUNDERING

3.1 ORIGIN AND TYPOLOGY
3.1.1 TRADITIONAL MONEY LAUNDERING
3.1.2 MODERN LAUNDERING TRENDS
3.2 A COMPLEX PHENOMENON
3.2.1 GLOBALISATION AND FINANCIAL LIBERALIZATION
3.2.2 FINANCIAL HAVENS – FROM JURIDICAL LOOPHOLES TO FINANCIAL BLACK HOLES
3.2.3 THE DUAL ROLE AND SOCIAL EMBEDDING OF ICTS
3.3 MAJOR MOVERS OF MONEY LAUNDERING COUNTERMEASURES
3.3.1 INITIATING LANDMARKS
3.3.2 THE FINANCIAL ACTION TASK FORCE
3.3.3 LAW ENFORCEMENT ENGAGEMENT: THE EGMONT GROUP
3.3.4 FINANCIAL SECTOR ENGAGEMENT: THE BASEL COMMITTEE AND THE WOLFSBERG GROUP
3.3.5 FRESH ARRIVALS: THE IMF AND THE WORLD BANK
3.3.6 ELECTRONIC AML

## 4 EXPLAINING AML EMERGENCE AND CONDUCT

4.1 INTRODUCTION
4.2 IDENTIFYING INTERNATIONAL AML AS AN INTERNATIONAL REGIME
4.3 THE MATERIAL AND SOCIAL EMBODIMENT OF INTERNATIONAL AML
4.4 EXPLAINING AML FORMATION AND PERSISTENCE
4.4.1 STATE POWER: THE ROLE OF THE USA
4.4.2 THE BENEFITS OF COOPERATION
List of Illustrations

**FIGURE 1**: THE THREE MONEY LAUNDERING STAGES .................................................. 33
**FIGURE 2**: A HYPOTHETICAL EXAMPLE OF POTENTIAL CYBERPAYMENTS ABUSE ............... 36

**BOX 1**: THE REGIME COMPONENTS OF THE INTERNATIONAL AML REGIME ..................... 55
1 Introduction

From late 1995 until 1999, as a vice president of Bank of New York, I agreed with my husband, Peter Berlin, and other people and entities to set up accounts at the Bank of New York for three entities, Benex, BECS and Lowland, for various purposes which were illegal under United States law. I did so to facilitate the movement of funds into and out of Russia, and to accomplish a number of objects which either knew were unlawful or deliberately closed my eyes to that I had reason to know was unlawful activity. I personally undertook various acts in order to further this illegal agreement.... In these transactions, I acted to benefit myself and my husband, and to develop more Russian business for the Eastern European Division of the Bank of New York.

- Former Senior Vice President of the Bank of New York Lucy Edwards’ admissions to money laundering crimes in Manhattan Federal Court.1

In 1998 the Bank of New York was put under investigation suspected of laundering 10 billion US Dollars for Russian organized crime networks via a company of which the executive manager was the Vice President of the Bank of New York Lucy Edwards’ husband. Edwards was the Eastern European Division Executive at the London branch reporting to the Eastern European Division Executive at the New York headquarters, Mrs. Kagalovskij. Her husband was at the time the International Monetary Fund (IMF) Executive Director for Russia and Vice President of the Russian bank Menatep, which through a shell company bought up the Russian oil company Yukos. The American correspondent bank of Menatep was the Bank of New York, which made profit from giving its Russian counterpart and other Russian banks access to the United States stock market by offering customer secrecy. As the case cracked, attention was directed towards Mr. Kagalovskij, suspected of laundering large sums for the Russian mafia via shell companies in financial havens. This money supposedly involved loans from the IMF to strengthen the Russian economy. Although Edwards was fired from her Bank of New York position and pleaded guilty to money laundering and unlicensed banking activity, she has still not been sentenced2, allegedly because she forfeited parts of the proceeds gained from the operations and has contributed to the investigation process.

1 http://www.russianlaw.org/crisis.htm
1.1 Money Laundering - The Scope of the Problem

For criminals to benefit from illegally obtained funds, the money must be integrated into the financial system and given the appearance of being legally acquired to avoid raising suspicion from law enforcement. Money laundering is defined as “the processing of criminal proceeds in order to disguise their illegal origin.”3 Although it obviously occurs outside normal economic statistics, the IMF estimates the sums laundered each year to be between two and five per cent of the global Gross Domestic Product (Gilmore 1999:21). By 1998 statistics this corresponds to sums ranging between 800 billion and 2 trillion US Dollars per year (Wechsler 2001:45). Money laundering is not a new phenomenon, but it has changed in the sense that it has increased in scope. The expansion of finance capitalism allows for world-wide capital flows in markets with few regulatory restrictions, a situation that can be exploited by actors involved in money laundering. A few transactions can move vast sums of money anywhere around the globe in the time it takes to press a few computer keys. The funds can then be concealed in financial havens operating with strategies of secrecy and anonymity, preventing governments from tracing dirty money.

The Bank of New York scandal is an example of sophisticated money laundering and illustrates how money easily can be relocated between bank accounts and jurisdictions via shell companies in financial havens. Accomplishment of the money transfers naturally involved dependence upon Information and Communication Technologies (ICTs) and more exactly on payment technologies4, and this is an example on how these technologies can be used in money laundering schemes. The scandal additionally reveals the actuality and presence of money laundering in an environment of poorly regulated law enforcement systems and corrupt financial officials exploiting banks to facilitate their own misdeeds, as represented by the top Bank of New York executives. This points in the direction of a lawless

---

4 “Payment technologies” will in this thesis refer to technologies supporting electronic transfer of value.
business culture undermining public confidence in national financial systems. The large sums laundered each year naturally call for an acceleration of countermeasures. Money laundering is recognized as a great problem requiring great response and has consequently become a top priority of the financial service industry and the authorities in most developed countries. The coordination of international anti-money laundering (henceforward AML) seems to be emerging within a formalized framework, leading to a set of questions that are central to this dissertation: Are international money laundering countermeasures coordinated enough to be labelled an international AML regime? If this is the case, then what are the main drivers behind the last decades’ growth in international efforts to curtail the problem? With regard to its ubiquity and globalisation, it is possible to identify a dual role of ICTs, without which the current money laundering dissemination most probably would be considerably less effective. How to these technologies, represented by electronic financial transaction technologies, serve both as facilitators of, and an auxiliary for fighting money laundering? The latter suggests that the technologies in question are attached to governmental needs and desires and must be treated as something socially embedded. Such indication of the technical characteristics of international countermeasures finally raises the question if the features of international AML are identifiable with a technological system. Does this affect AML policies?

1.2 Money Laundering Countermeasures- The Scope of Response to the Problem

Since the late 1980s concerted action has been taken in large parts of the world to build coordinated international initiatives to combat money laundering as threats posed by international drug trade became a central issue of concern (Gilmore 1999:13). Initiated by two landmarks in 1988, the Vienna Convention and the Basle Committee Statement of Principles, both grounded in US concerns with increased trade in narcotics and abuse of the banking system for the purpose of money laundering respectively, a growing network of states and
international bodies including the UN, the OECD and the EU has established common regulatory international AML standards. Perhaps the most important achievement has been the G7’s\textsuperscript{5} creation of the Financial Action Task Force on Money Laundering (FATF), the most important contributor to international AML in charge of developing and promoting policies to combat money laundering by bringing together the policy-making power of legal, financial and law enforcement experts (Carlson 2000:129). Achieved establishments comprise institution building and cooperation in adopting investigation, prosecution and prevention techniques including reporting requirements of suspicious transactions, record-keeping and information sharing built on an underlying principle of transparency. Implementation of established standards is encouraged through peer pressure, technical assistance and monitoring, and sanctioning methods are employed if AML requirements are not complied with (130). A method that was conducted by the FATF in this respect was a naming and shaming strategy in 2000 pushing through regulatory compliance on non-cooperating actors. This black-listing was however abandoned by 2003 (Sharman 2004:1). Countermeasures have been additionally enhanced after the terrorist attacks of September 11\textsuperscript{th} 2001 in New York and Washington. When linkages were discovered between money laundering and the financing of international terrorism the commissions of the FATF were immediately expanded. Since then international AML has taken on a new form through the war on terror, grounded in a desire to control the uncontrollable: to predict possible terrorist attacks that are by their nature unpredictable (de Goede 2004:3). This new way of targeting money laundering and terrorist financing builds on preventive surveillance of financial transactions inter alia as to detect anomalies (de Goede 2004). Such a predictive technological intelligence strategy is a product exemplary of the risk society\textsuperscript{6}. Apart from assessing possible terrorist attacks, the objectives behind international countermeasures are to remove profit from criminals by denying them

\textsuperscript{5} Although the G7 has been changed to the G8, G7 will be the term employed in this thesis.

\textsuperscript{6} The concept of “risk society” refers to the idea that society is exposed to socially created risks.
the ability to launder illicit gains, and to identify and prosecute them, based on the assumption that criminals will not want to take the risks involved if they do not benefit from their actions (Carlson 2000:128). It is however a controversial issue due to the trouble of finding the balance between a legitimate minimum of participation by all parties and a strong enough element of top-down policy from powerful states to make it successful (Tranøy 2003:4).

1.3 Motivation: Money Laundering in Context
The reasons for targeting money laundering include a wide range of negative impacts not only on the economy, but on society in general. The IMF stresses that money laundering leads to “inexplicable changes in money demand, greater risks to bank soundness, contamination of legal financial transactions, and greater volatility of international capital flows and exchange rates” (Wechsler 2001:45). Economic effects are not the only reasons for concern. An underlying worry is the encouragement of corruption and bribery giving criminals influence in banking institutions (Tsingou 2004:4). For laundered money to enter the legal financial system, it is often necessary to bribe bank officials to avoid law enforcement suspicion. This complicates unveiling of the affair, since lack of information sharing hampers detection. Detecting money laundering gets even more hampered when banking officials are themselves part of the game. The Bank of New York story illustrates this. Top executives of acknowledged financial institutions\(^7\) exploited legal financial structures for personal gains through corrupt behaviour. Such corruption of credible institutions leads to a loss of honourable authority in the financial sector, which is an unwanted situation in an international environment where increased cooperation based on information sharing is considered a necessity in preventing financial crimes. As reflected in the expanded commissions of the FATF after September 11\(^{th}\) 2001, money laundering also poses problems to national security

---

\(^7\) The term refers to persons or entities conducting deposit acceptance, lending, leasing, transfer of money or value, issuing means of payment, diverse trading and other financial commitment as a business for or on behalf of a customer. For a more detailed definition see appendix C.
because of the alleged linkages to international terrorism. This indicates a change in the nature of international security politics, moving from purely military questions towards the inclusion of economic issues of concern.

AML initiatives must also be seen in relation to the violent crimes often underlying money laundering. The recognition of the establishment of a global network of criminal activities is often referred to in a collective term as a “criminalization syndrome”. The term treats transnational organized crime including drug trafficking, trafficking of women and children for commercial sex, arms trafficking, illegal markets, corruption, rent-seeking and money laundering as closely related and mutually reinforcing phenomena (Williams & Baudin-O’Hayon 2002:128). The growth in organized crime has made money laundering an important part of the game, since criminal proceeds must be concealed. The criminal element to money laundering is thus twofold in the sense that it stems from a crime and enables criminal activity to be maintained.8

1.4 Objectives and Research Question

Money laundering has increased in scope and taken on new forms. In many cases this diminishes reliance upon corrupt financial officials, partly because internet banking from home reduces the role of face-to-face contact and removes third party liabilities. Legal financial transactions have a link between the funds and the persons involved. Money launderers therefore desist from using normal payment systems and rely on cash, which offers anonymity (Molander et al. 1998a:5). But physical movement of large amounts of cash is risky, and advances in payment technologies can remove this burden. “Cyberpayments” is a collective term for these new techniques describing a “class of instruments and payment systems that support the electronic transfer of value”, which can take place via the internet or through stored value smart cards (11). They reduce transaction costs and increase transaction

efficiency, but are vulnerable to exploitation by criminals. The global nature of these systems also enables criminals to take advantage of different national regulations; however, this does not imply that laundering money is easy. On the contrary, enhanced regulation and coordinated international response to the problem increases the costs and risks of money launderers to continue their activities, and as these countermeasures reach wider geographical circumference, there will be fewer loopholes to exploit. Moreover, AML participants use payment technologies as a source of information, and rules requiring surveillance of transaction technologies have been implemented in many countries. In particular, AML after September 11th 2001 defer to intensive surveillance technologies based on financial transactions designed to intercept suspicious activity. This leads to the main objectives of this thesis which are to:

- Investigate if international AML can be identified as an international regime, which also possesses the features of a technological system that influences AML policies
- Present the driving forces behind the last decades’ increased coordinated international initiatives to curtail money laundering
- Demonstrate that developments in ICTs play a dual role in the sense that they are used both for the purpose of money laundering, as will be demonstrated by the techniques and strategies involved, and for the purpose of combating it, as is evident by the technical character of international AML

These objectives can be summed up in the following research question:

*Can international AML efforts be identified as an international regime possessing the features of a technological system, and how can the proliferation of payment technologies be used both to facilitate and fight money laundering?*
1.5 Methodology

The use of payment technologies in money laundering and AML schemes calls for the presence of ideas from the Science, Technology and Society (STS) school of thought. A view often put forward in the globalisation debate is that of technological determinism, which in its most extreme forms considers technology as something autonomous outside of social context causing social change (MacKenzie & Wajcman 1992:2). As such, electronic payment technologies have been blamed for causing money laundering to increase in scope. A counter argument is that it is not the technology itself that causes change, but the underlying social factors involved. This emphasis on the social embedding of and influence on technology is a fundamental principle in the STS literature (Wyatt 1998). It does not imply that technologies do not affect social change, but rather social structures such as social interaction, norms, needs and desires influence technological change by linking technology and society. To understand the dual role of ICTs in relation to money laundering, perspectives from the STS literature will be very helpful. In the AML context this means that international cooperation can be influenced by the underlying AML technologies used in pursuit of political goals and vice versa. The international project of combating money laundering is a complex issue, and comprises a myriad of international bodies and organizations. Despite their role as important contributors to international AML, all actors engaged in the AML campaign can not be emphasized in this thesis. Rather, importance will basically be attached to the bodies that are most relevant to the analysis. This does not mean that the excluded participants are less relevant; on the contrary, there are organizations that in certain areas have contributed more in the fight against money laundering than some of the bodies referred to here.

Engagement with the theoretical basis has been sought carried out following the guidelines of Chris Hart’s “Doing a literature Review” (1998). In seeking a relevant theoretical framework for the analysis I ended up combining two different theories to explain the growing international response to money laundering. These are regime theory and the theory
of technological systems. Regime theory is a commonly acknowledged approach in the literature on global governance and international relations, and can be classified in three schools of thought explaining the driving forces behind international cooperation (Hasenclever et al. 1996:178). (1) Power-based realist approaches focus on the distribution of power resources between states. The core of this approach is the hypothesis of hegemonic stability, which emphasizes the crucial role of a strong dominating actor in international politics in order to realize collectively wanted outcomes. (2) Rationalist interest-based theory describes how international regimes help states realize common interests by serving as a tool for simplifying international cooperation through mutually adjusted behaviour useful to all parts. Finally, (3) knowledge-based theories placing discourse, ideas and learning at the centre see international regimes as a social phenomenon in which actors’ notion of the world is formed through international interaction (Stokke & Claes 2001). A commonly used definition developed by Krasner treats international regimes as “explicit or implicit principles, norms, rules and decision-making procedures around which actors’ expectations converge in a given area of international relations” (Hasenclever et al.1996:179). Taking into account the structure, diffusion and implications of international money laundering countermeasures, regime theory is highly relevant to the analysis.

A recent approach to international collaboration has been developed by Porter drawing on Hughes' theory of technological systems, referring to a system of embedded knowledge created by people. In issue areas where such systems exist, these “can shape the conduct of actors involved in international institutions in ways that other approaches to international institutions, such as regime analysis, overlook” (Porter 2003:521). To illustrate this Porter refers to three features of technological systems that can shape actors’ conduct. These are material embedding, complex path dependence and technical authority. Porter’s approach does not oppose power-, interest- and knowledge-based theories, but focuses on how technical
features associated with technological systems can affect the way international politics operate, and is thus complimentary to traditional regime theory. It may be applied on international AML and seems particularly relevant in explaining the post September 11\textsuperscript{th} 2001 risk based collaboration strategy characterized by a preventive search for unusual transaction activity based on technologies designed to detect anomalies.

The theoretical platform of the analysis combining traditional regime theory with Porter’s application of Hughes’ theory of technological systems enables me to give a thorough account of the driving forces behind, and a description of the characteristics of, coordinated international AML efforts. To understand the most commonly employed techniques used in money laundering processes, and techniques used to counter money laundering, it is necessary to study advances in ICTs developed for the financial system. Central to this is the already mentioned cyberpayment system including internet services and the use of payment cards, but also traditional banking transaction systems will be taken into account. It will be described how electronic payment technologies also can be used for the purpose of curtailing money laundering. To avoid adopting a position of technological determinism in this respect it will be central to emphasize the social embedding of these technologies, something that places me within the broader framework of the SCOT (the Social Construction of Technology) school.

The empirical basis of the thesis is to a large extent based on reports, papers and typologies carried out by the main international AML bodies. As a matter of course, taking the objectives of the thesis into account, it was useful to approach people working against money laundering on a daily basis. To reinforce the empirical data basis, I therefore conducted a series of qualitative interviews with AML professionals. Taking account of the time and resources available, the number of interviewees came down to seven. According to Hammersley and Atkinson, in ethnographic research the aim is often to select a sample of interviewees who are representative to the research. But a representative sample is not always the objective,
particularly in cases where the goal is to gather information rather than document perspectives. The aim of my interviews was precisely to “target those people who has the knowledge desired and who may be willing to divulge it to the ethnographer” (Hammersley & Atkinson 1995:137). All the informants were professionals engaged in combating money laundering, and their expertise offered an exclusive source of information. Their expertise as source of information is also a reason why it was not necessary to interview a large sample from which a comparative analysis could be conducted. To cover all aspects of my objectives, I selected two representatives from the technology sector engaged in the development of software solutions to unveil money laundering, two representatives from the law enforcement sector; one special adviser from the Financial Supervisory Authority of Norway (Kredittilsynet) and one from the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim), one representative from the financial sector; the Norwegian Financial Services Association (FNH), and the Norwegian FATF delegate. I also interviewed one former law enforcement official with the underlying objective of getting a perspective on money laundering that was not bound to the interviewee’s professional position. This is in accordance with Hammersley and Atkinson, who claims that it is sometimes more effective to talk to people who has “left office”, since they can more freely offer inside information (Hammersley & Atkinson 1995:138).

To get in touch with the interviewees, I attended a money laundering seminar where I came in contact with people who served as gate openers by recommending persons it would be useful for me to talk to. As such, I found the process of selecting relevant interviewees quite painless. I conducted semi-structured interviews of one hour endurance. It must be stressed that the analysis of the contents of the interviews are based on my interpretation of the interviewees’ accounts, and that accordingly, it can not be guaranteed that there are no incongruities between the interviewees’ opinions and my analysis. Thus, the persons whom I
talked to can not be held responsible for the arguments presented in this thesis. Due to the different professional positions of the interviewees, it was also reasonable to emphasize different topics depending on whom I talked to. The interviews were recorded, something that allowed me to concentrate on the accounts given by the informants, to support a natural course of the conversation. Although the interviews were fairly non-directive, they were structured in the sense that I entered them with a list of key topics to be covered, even if these did not follow a structured order. The interviews were transcribed immediately after each interview. This was favorable in the sense that it allowed me to simultaneously write down interpretative notes while I still had a fresh memory of the conversations. A summary was then made to each interview and coinciding perspectives are emphasized in the analysis.

1.6 Thesis Structure
The next chapter presents a review of the analytical tools used in the analysis. Three regime theory approaches are presented, which offer different but complimentary explanations to why states cooperate, how international regimes emerge and how cooperation within regimes is maintained. The chapter also introduces a technological systems approach and argues that the technical features of an issue area can shape international AML. Expected findings are listed at the end of the chapter.

Chapter three starts with a description of money laundering, what it is, its origins, the stages of it and common techniques. It is seen in light of globalisation and financial liberalization and the extensiveness of financial havens, which is considered crucial to understanding its dissemination. The chapter also describes the social embedding of technologies by drawing on perspectives from the STS school of thought. In this respect, the major bodies behind international AML are introduced. The features of the policy frameworks presented by these bodies reveal a dual role of ICTs in the sense that the same technologies vulnerable to exploitation by criminals can be used to target money laundering.
Chapter four determines if international AML can be labelled an international regime. It further investigates if international AML possesses the features of a technological system, and the degree to which the technical features of money laundering countermeasures have an impact on AML policies. An explanation will be provided to the reasons why coordinated action has been initiated against money laundering. Empirical data is linked with the theoretical approaches, and it will be demonstrated that the various theories are relevant at different stages of AML. The findings are finally drawn up in chapter five.
2 Collaboration: International Regimes versus Technological Systems

The aim of this chapter is to identify the analytical tools necessary for me to be able to answer the following: Does there exist an international regime to combat money laundering? If it does, then how can its emergence be explained? If it does, are the features of this regime identifiable with a technological system? In that case, how does this affect AML policies?

An important feature of globalisation has been the creation of regimes to govern international relations, although theorists hold divergent views as to how and why regimes are created and maintained. Whereas people who hold a pessimistic view of globalisation doubt that it is possible to manage globalisation, regime theorists are optimistic and agree that the ability to benefit rather than suffer from it, depends on the “capacity to regulate global activity by means of regimes” (Little 2001:305). Regimes persist inter alia in areas of international security, in the regulation of environmental issues and of the international economy. Interest in studies of the regulation of state behaviour has subsisted since the emergence of the state system, but the regime concept is of relatively recent origin and was introduced by social scientists in the 1970s.

2.1 Defining an International Regime

The regime concept has been debated among theorists, but the most widely used definition is that of Krasner (1983:2) who identifies regimes as “sets of implicit or explicit principles, norms, rules and decision making procedures around which actors’ expectations converge in a given area of international relations”. By studying the four regime components separately it is possible to dismantle this definition. Principles are general formulations of objectives and basic casual understandings represented by bodies of theoretical statements about how the world works. Norms describe rights and duties of states and specify general standards for behaviour, whereas rules are specific directions for behaviour at a lower level of generality.
than the two former components, often designed to conciliate existing conflicts between principles and norms. Together, principles, norms and rules constitute the substantial part of a regime. Many regimes additionally hold a fourth operational component; procedures, which identify agreed practices to ensure rule establishment and implementation. These will change when the regime is consolidated and extended (Stokke & Claes 2001).

Hasenclever et al. point out a number of implications of Krasner’s definition. Arguing that “Regimes are a special case of international institutions and should be studied as such” (Hasenclever et al. 1996:179), they stress that international regimes must be treated separately from international organizations, which are formal physical unit characterized by its mandate, localization and staff, often forming the central operational element in multilateral regimes. Further, regimes must be separated from negotiations, which are limited by case and lack a substantial core of recognized rights, duties and norms. Finally they must be separated from conventions; sharing with regimes the assumption that actors’ expectations centre on specific norms, but members of regimes do not always wish to carry out the norms if there are others who do (Stokke & Claes 2001:271). Other implications that are more controversial concern the meaning and distinction of the four regime components, as well as the phrase “around which actors’ expectations converge”, where the problem is to know when a regime actually exists in an issue area (Hasenclever et al. 1996:179). Despite these implications, Krasner’s definition will be the one referred to henceforward and if it is applicable in practice in the AML context, the regime components should be identifiable within international efforts to target money laundering.

The relevance of international regimes relies to a large extent on their effectiveness. If the regime does not contribute to solve the problem that motivated regime formation in the first place, its relevance will be questioned. Hveem (2001) refers to a number of regime features that are regarded important in this respect. First, regimes must be built on voluntariness as far
as attendance is concerned, but must simultaneously hold the possibility to perform some kind of sanctioning towards members who do not play by the rules, thus a balance between compulsion and voluntariness must be maintained. Moreover, rules and laws are not sufficient to secure successful cooperation, and there must be elements of learning and maybe also self-interest (Hveem 2001:105). International AML does however challenge the emphasis on voluntariness because the FATF seeks to enforce compliance in both member and non-member countries, exemplified by the black-listing of non-cooperative actors.

2.2 Three Schools of Regime Theory
In the following, theoretical explanations will be given to why and under what conditions states agree to cooperate by developing institutions which might affect their alternatives of action. It is common to distinguish between three main approaches to regime theory. The first, power based theories, are rationalistic and emphasize the distribution of power between states. The second approach, interest based theories, is also a rationalist approach trying to reveal how international regimes can make it easier for states to realize common interests. Third, knowledge based theories regard international regimes as socially constructed phenomena and place discourse, ideas and learning at the centre (Stokke & Claes 2001:273).

2.2.1 Power Based Theories
Power based theories emphasize the distribution of power between states. A central aspect of this approach is the hypothesis of hegemonic stability. It refers to the presence of a hegemon; a strong, dominating actor in international politics which is important in order to realize collectively wanted outcomes. A hegemon possesses power resources. These resources serve as a pretext to make other countries adhere to the will of the hegemon by complying with commitments in international regulations (Stokke & Claes 2001:277). In order to make other countries comply, the hegemon can choose between persuasive means like inducements and promises, and coercive means like sanctioning or threats of sanctioning (Hveem 2001:111).
According to the hegemonic stability hypothesis, when the regime ceases to maintain the interests of this main actor, it is likely to collapse. The hegemonic stability thesis has however been criticized for not holding satisfactory evidence and tends to ignore other analysis than extreme power constellations (Stokke & Claes 2001). Moreover, the presence of a dominating actor is neither necessary nor enough in the establishment of an international regime (Hasenclever et al.1996:198).

According to Little (2001:301) the impact of regimes on international relations is that it will “facilitate co-ordination of policies and actions but only insofar as this does not alter the balance of power among states”. Coordination is here defined as “a form of cooperation requiring parties to pursue a common strategy in order to avoid the mutually undesirable outcome arising from the pursuit of divergent strategies” (314). Cooperation is thus a conflict of distribution of who gets what and according to Krasner this conflict can be solved by the use of power in three ways (Hasenclever et al.1996:200): (1) to determine who is allowed to play the game: less powerful actors are often not invited to join the game, (2) to dictate the rules of the game: the most powerful actor gets to dictate the outcome, and (3) to manipulate the outcome of regime formation: the most powerful player can manipulate others’ preferences with threats or promises.

Following the above account, when analyzing international money laundering countermeasures, it can be expected that the power based approach will manifest itself in relation to the initiating stages of AML cooperation. It should further be possible to identify a dominating actor encouraging regime establishment. It is commonly acknowledged that the USA is a hegemonic actor in many respects. An example of a US power resource is that they have the biggest financial market in the world. This US share of the world’s financial markets should indicate that the extensiveness of money laundering affecting the USA is correspondingly large. An incentive is thus created for using its powerful position to push
through international collaboration against the problem. If countries depending on business with the USA are denied access to their markets the consequences would be severe, thus it would be likely that international agreements would be adopted. Moreover, due to the influence of the USA in initiating the fight against money laundering, as exemplified by the establishment of the Vienna Convention and the Basle Committee Statement of Principles in 1988, the hypothesis of hegemonic stability can be expected fortified in the AML context. In consistence with Krasner’s three ways in which states can use their power, the dictating of regime outcome through threats and promises should be ascribed to the USA. However, the hegemonic power in international AML does not immediately point to any particular country, rather it calls for the position of the FATF due its role as a standardizing AML body. Yet as a forum put together by the countries of the G7 it is likely that the power of the FATF reflects the will of the most powerful countries within this ensemble. Following the above indication it can be expected that the work of the FATF largely reflects US desires.

2.2.2 Interest Based Theories
Interest based and power based theories are both rationalistic and treat states as the most important actors in international relations (Little 2001:301). However their assessments of regime analysis are competing. As US hegemony was on the decline on the international scene in the late 1970s, explanations of regime persistence had to be sought elsewhere than by the hypothesis of hegemonic stability. With his book *After Hegemony* (1984), Keohane, a leading contributor to the interest based tradition, asks if international regimes can persist in the absence of a hegemonic power. He concludes that they can because international regimes are created because they are expected to ease cooperation, and that common interests are best realized through mutually adjusted behaviour in order for all actors to benefit from it (Stokke & Claes 2001:274). Keohane emphasizes three functions a regime can maintain (Stokke & Claes 2001:274). Keohane emphasizes three functions a regime can maintain.

---

Claes 2001). One is the establishment of patterns for mutual liability, referring to recognized rules for behaviour which will create mutual expectations about each other’s conduct even if these rules are not subject to law enforcement. Actors will accept the costs of regime establishment in return for the expected advantages. The likelihood of regime creation thus augments if the “potential mutually beneficial agreements in the issue-area is large” (Hasenclever et al. 1996:186). The second function is the distribution of information. Cooperation is easier when states share information about goals and interests. This reduces information costs and makes it easier to form a basis for agreements that otherwise might be hampered by the insecurity of other’s intentions (Stokke & Claes 2001:274). As noted by Hasenclever et al. (1996:186), if regimes secure availability of information about each others’ compliance through monitoring arrangements, “they reduce the fear of being cheated”. If they additionally have procedures for collecting information on compliance this may reduce the fear that others dodge the agreements entered into (Stokke & Claes 2001:275). Besides, actors’ awareness of the detection probability by breach of contract, and the probability that the actors will meet again in future negotiations, increases incentives for engaging seriously with the commitments (ibid). Cost reductions of negotiating international agreements is the third central function of regimes. Negotiating several agreements between several countries is more resource demanding in terms of time, communication, information sharing and decision making than negotiating a common framework (Hveem 2001:109). The regularity of meetings and the comprehensiveness of participation of regimes make it easier for actors to come together and reach consensus than it would have been to negotiate a set of bilateral agreements. The costs of negotiating a common framework and the complexity of this framework in turn contribute to regime persistence (Hasenclever et al. 1996:187).

Keohane developed his theory within a framework of the Prisoner’s Dilemma illustrating the need for a collaboration strategy to show how regimes can influence actors’ ability to
cooperate. Collaboration is here referred to as “a form of cooperation requiring parties not to
defect from a mutually desirable strategy for an individually preferable strategy” (Little
2001:314). The Prisoner’s Dilemma describes interaction between two actors having two
possible strategies each; cooperative and competitive. The juxtaposition of preferences reveals
that infringing agreements may be the best strategy to pursue regardless of what other actors
do (Little 2001:308, Hasenclever et al. 1996:183). Because both actors expect the other to
choose competitive strategies, states fail to pursue collaborative strategies and miss an optimal
outcome (Stokke & Claes 2001, Little 2001), but international regimes can be an instrument
to overcome this dilemma.

If the interest based approach is relevant to the analysis, it can be expected that fighting
money laundering is considered a common interest. This should be rooted in a recognition
that targeting money laundering is more beneficial through international collaboration than it
is to counter the phenomenon individually. Because of the crucial role of the FATF in
international AML, it can be expected that the task force can replace the missing hegemon in
developing a possible regime. If this is the case, Keohane’s three regime functions, mutual
liability through recognized rules for behaviour; mutual information sharing and regime
maintenance owing to cost reductions through comprehensive cooperation, are likely to be
upheld under direction of the FATF.

2.2.3 Knowledge Based Theories
Cooperation does not necessarily have to be understood in light of the self-interest of rational
actors, but can also be understood in terms of knowledge. Knowledge based theories place
discourse, ideas and learning at the centre and criticise rationalist theories for not taking into
account that the countries and organizations involved in international relations consist of
people with individual meanings. They are constructivist in the sense that they stress that
regimes must be seen as social phenomena arising as a reflection of the identities and interests
of states and groups which are in themselves forged through interaction (Little 2001:296, Stokke & Claes 2001:278). As not to black box the meaning of the term “learning”, it will here be understood as a “process through which collective behaviour is modified in light of new collective understanding” (Haas 1994: 41). This emphasis links this approach to central ideas of the STS school of thought.

Consensus must be reached about the issue area at stake before states can agree on how to deal with it. Such consensus may be achieved after a process of learning. This calls for the hypothesis of epistemic communities, which is the pillar of knowledge based theories. Due to politicians’ inability of assessing the outcomes of their decisions, they call for scientifically reliable information (Hasenclever et al.1996:206). Epistemic communities refer to “networks of knowledge-based communities with an authoritative claim to policy-relevant knowledge within their domain of expertise” (Haas 1994:45). This knowledge does not appear in isolation, but is “created and spread via transnational networks of specialists” (44). These experts can be politicians, diplomats, entrepreneurs and scientists, and they are crucial because if ideas and knowledge are to have an impact they must be commonly shared (Hasenclever et al.1996:209). The point is that these experts share a common understanding of the causes and characteristics of the problem at stake and agree on how the problem is best solved. Consensually shared knowledge is however not always guaranteed in international cooperation. In such situations compliance can be ensured by a hegemon in the issue area (216). According to Haas, epistemic communities influence regime creation and maintenance because negotiations succeeding policy innovations are conditioned by the information provided by the epistemic community. They also influence policy diffusion. Advances in modern communications and increased access to information allow epistemic communities to operate transnationally, and this international expert share of information can in turn affect their respective governments (209).
If there exists an international AML regime, is it possible to identify a network of experts providing scientifically reliable information relevant to regime policies? If it is, it should be possible to identify an influence of such epistemic communities on regime formation and evolution. Moreover, evidence of epistemic communities should be found within the FATF and its surrounding network of international bodies engaged in combating money laundering. International AML standards including the FATF 40 Recommendations and other FATF documents should in this case be based on a certain degree of consensus knowledge before being presented as directions for behaviour.

2.3 Technological Systems
According to MacKenzie & Wajcman (1992:12) “technologies come not in the form of separate, isolated devices but as part of a whole, as part of a system”. A contemporary approach to such systems, the technological systems approach, has been developed by Hughes, demonstrating in his Network of Powers (1983) and The Evolution of Large Technological Systems (1993) how technologies are embodied in systematized knowledge with cultural, social, political and economic dimensions. At the heart of this approach lies a refusal to deal with the technological and the social separately (Bijker et al. 1993:196). This suggests that technological systems are socially constructed but also society shaping, which reveals close linkages to the knowledge based approach of regime theory. Hughes has identified specific system components including physical artefacts, organizations, scientifically labelled components as well as legislative artefacts, and uses the electricity power system as an example: Physical artefacts refer to turbo generators and transmission lines, organizations refer to firms and investment banks, scientific components can be articles and research programs and legislative artefacts refer to regulatory laws (Hughes 1993:51). By applying Hughes’ theory of technological systems on the regulation of the international financial system, Porter has modelled an approach demonstrating that where there exists a
technological system, it “can shape the conduct of actors involved in international institutions in ways that other approaches to international institutions, such as regime analysis, overlook” (Porter 2003:521). Referring to technological systems as “spatially extended and functionally integrated socio-technical networks” (522), his argument is that the technical feature of an issue area can influence international cooperation. This opposes a rationalist emphasis on the choice among alternatives, because according to the technological systems approach, in technology intensive issue areas these alternatives are shaped and constrained by technical factors associated with this system (524), but the technological system can also be used in reaching desired goals. Porter operates with three indicators of technological systems which may influence actors’ conduct. These are material embedding, complex path dependence and technical authority. Material embedding refers to how physical components of technologies by being applied are integrated with social dimensions, and this can produce patterns for regulated activity. Second, Porter claims that the need for coordination of the system components can stimulate established patterns for “institutional practices” (523). Once these patterns gain foothold this can secure regime maintenance, and is what Porter refers to as path dependence. In his words, the logic of technological systems is that

Decentralized practical technical international arrangements precede, stimulate and shape high level political negotiations and these negotiations then seek to resolve problems from the prior technical collaboration through new institutional innovations. These new institutional innovations will build on the earlier technical arrangements (Porter 2003:527).

Third, technical authority relates to the importance of scientific and technical expertise as a key source of generating authority, and refers to how compliance is based on the integrity of the source of rules rather than being based on self-interest and compulsion. This integrity is secured through the performance-based orientation of technical authority, which is also oriented towards practical relations that do not principally focus on politics. Moreover,
technical authority is open to criticism, revision and input from technical experts, and this may increase the legitimacy of this source of authority (523).

It is important to notify that Porter does not reject the role of traditional regime theory, but stresses that these approaches are modified in interaction with the technological systems approach in issue areas where such systems exist (540).

A potential weakness of Porter’s theory is that due to its resemblance to the already established regime theory, his contribution can in many respects call on the Emperor’s new clothes metaphor. Most of his accounts can be explained by either power, interest or knowledge based theories, thus it may be difficult to spot an obvious relevance to the analysis. However, if international AML can be identified as a technological system, Porter’s account contains aspects which probably can offer explanations that are more suitable for international AML than traditional regime theory. I hereby present a proposition saying that if international AML possesses the features of a technological system, it must first of all be possible to identify Hughes’ system components. These components may exists independently without there being a system, therefore, it will be argued that the presence of Porter’s concept of material embodiment is crucial as to link the system components together for there to be a technological system to speak of. The influence of a potential technological system on international AML will in turn be explained by Porter’s account of path dependence and technical authority.

The presence of technical features like the mentioned monitoring of financial transactions in order to detect suspicious activity based on technologies designed for this purpose not only suggests that international AML is a technology-intensive issue area but gives a hint of scientific components as well. Combined with the ensemble of bodies engaged in combating money laundering as well as AML rules that have been implemented in many countries, it should not be difficult to identify Hughes’ system components. Material embodiment should be
found in some kind of interaction between these system components, for instance a dependence on electronic networks. The relevance of this technical approach is particularly likely to manifest itself in explaining AML after September 11th 2001 and the onset of a risk based intelligence strategy based on preventive surveillance of financial transactions. This risk based approach can be seen as a product of the risk society; the idea that society is exposed to socially created risks, and is “characterised by a cultural desire to tame chance and effect security, and by institutions increasingly organised around risk management” (Ericson & Doyle 2004:41 in de Goede 2004:3).

Path dependence can be linked to the interest based theory and Keohane’s assertion that once a regime is created it will persist due to the costs of creating it. Porter’s notion of path dependence seems to be rooted in what Hughes refers to as momentum and trajectory in his works. Because of an interrelatedness between physical and social system components, once consolidated technological systems gain momentum. For instance, companies, laboratories and regulatory bodies amplify the momentum of electric power systems, and inventors, scientists and politicians have vested interests in this systems’ persistence (Hughes 1993:77). At the early stages of application of new technologies, human actors like scientists and engineers can control its usage and progress. But as the system gets entangled in society over time its prevalence becomes predominant (76-80). This merging of technological determinism and “social determinism” that Hughes’ account insinuates can explain actors conduct at two levels. In prolongation of the feature of material embodiment, an expected dependence on electronic networks in combating money laundering could possibly be explained by the momentum these technologies have acquired in the financial system. Second, it can be expected that the momentum gained by international AML can explain regime persistence more specifically than Keohane’s account. In the analysis the term path dependence will be used instead of momentum.
Technical authority has strong linkages to Haas’ epistemic communities concept. But a distinction between the two can be identified. Haas’ notion of scientific knowledge seems to be rooted not only in science, but includes political ideas and opinions as well. It takes into account the influence of social conventions, irrespective whether they have emerged out of scientific, cultural or political factors. Technical authority on the other hand, seems to be based more exclusively on scientific knowledge independent of prevailing ideological political ideas in the issue area at stake. This independence can provide breeding grounds for consensus knowledge in international cooperation. Its openness to criticism and revision suggests that technical authority may be perceived as a bottom-up expertise, whereas scientific knowledge of epistemic communities to a larger extent reflects top-down expert knowledge. If international AML has the features of a technological system, possibly Porter’s technical authority concept has more explanatory value than the notion of scientific knowledge related to epistemic communities. In this case it can be expected that AML standards are grounded in such “democratic” knowledge.

2.4 Summary of Expected Findings
Having presented the analytical tools for the analysis, the major tasks that are to be carried out can be summed up. First of all, can international AML be identified as an international regime? An answer to this will be provided by examining Krasner’s regime components: is it possible to identify specific principles, norms, rules and procedures through which international money laundering countermeasures are operationalized? The extensive framework of AML policies to be implemented in FATF member and non-member countries suggests that it is, and it can be expected that these regime components are recognizable within FATF provisions. The next task will be to examine what characterizes the international AML nexus. What kind of regime does international AML possibly represent? As demonstrated by Porter’s application of the technological systems approach, in issue areas
where there exists a technological system, international cooperation can be conditioned by the technical features of the issue area at stake. Extensive use of payment technologies in money laundering schemes and a dependence on information gathered from these technologies in combating the problem indicates the technical characters of international AML. But does it also possess the features of a technological system? This assumption will be strengthened if empirical evidence shows that Hughes’ system components are present in the AML nexus, but only insofar as evidence of Porter’s material embodiment concept as a means of sticking these components together additionally is provided for. As indicated above it is likely that these requirements will be fulfilled. In particular, it can be expected that the feature of material embodiment is particularly obvious in explaining the risk based approach adopted after September 11th 2001.

The final task is to give an account of the driving forces behind international AML. In less than two decades an increasing number of countries have adapted to the regulatory framework provided by leading international AML bodies. What explains so many countries’ compliance with international AML standards? I will provide an answer to this by applying the three regime theory approaches and the technological systems approach on international AML. Although these approaches are divergent in many aspects, they must be treated as complementing rather than competing. All three possess value but none of them seem sufficient to explain regime formation and maintenance alone because they set different preconditions for how international cooperation should be understood. It will be demonstrated that elements from all approaches are useful in explaining the dynamics of international AML. The degree of relevance of the different approaches can be expected to vary depending on the different stages of the AML process. Viewed in the light of the presented theoretical perspectives, did international AML arise in response to a hegemonic actor using its power to promote collaboration? Taking into consideration the indicated role of the USA in
international AML, it can be expected that regime formation grew out of US interests. Keohane stressed that regimes also can persist in the absence of hegemonic actors if it is commonly recognized that collaboration in an issue area is more beneficial than it would be for countries to deal with this issue individually. Do countries jointly acknowledge the benefits of collaborating against money laundering? If such consensus is traceable it can be expected that the dictating of regime outcome consistent with Krasner, and the three regime functions consistent with Keohane, is maintained by the FATF. Following the knowledge based tradition, AML collaboration should reflect prevailing ideas, norms and knowledge commonly shared by a group of experts exemplary of epistemic communities. Is international AML characterized by such epistemic communities whose expert knowledge has influenced AML policies? Or is Porter’s concept of technical authority more prevalent in this respect than Haas’ hypothesis of epistemic communities? Or do the two concepts prevail at different stages of international AML? Is AML collaboration characterized by a choice of alternatives consistent with rationalist theories, or is it path dependent; is it subject to the momentum acquired through its own evolution?

The next chapter described how ICTs are used to facilitate and counter money laundering. It starts with an examination of money laundering techniques and typologies, and factors that are important to understand the dissemination of the phenomenon are briefly discussed. The last part of the chapter presents major bodies engaged in international AML. This account will serve as the starting point on which the analysis is built.
3 Facilitating and Fighting Money Laundering

“Globalisation has turned the international financial system into a money launderer’s dream.”
-Pino Arlacchi, Executive Director of the UN Office on Drugs and Crime, 1998.

3.1 Origin and Typology
Proceeds generated from illicit activity are of little use to criminals if the origins of the money do not avoid law enforcement suspicion. The money trail must thus be disguised. The term “money laundering” illustrates what happens: cleaning dirty money. It is the process through which illegally obtained funds is given the appearance of having originated from a legitimate source. The reason why criminals want to disguise these proceeds is twofold: first, because the money trail in itself can become evidence of the crime; and second, because the money is vulnerable to seizure and can become target of investigation (Blum et al. 1998:4).

Money laundering is not new. The origin of the term dates back to the 1930s when the mafia in the USA bought up cash based laundry halls with which illicit proceeds could be mixed to make it appear as legally obtained. Cross border money laundering goes back to the 1960s and the outset of financial liberalization, when the opportunities to exploit the financial system increased. By opening bank accounts in financial havens, illegally earned income could be hidden in other countries (Helleiner 1999:4), thus opening up for an expansion of the activity. Today’s reach of money laundering must be treated as a global phenomenon. In a flash, large sums can be repeatedly relocated between bank accounts almost anywhere in the world via cross border transactions in a “borderless” financial network. Such a view of state border elimination is however somewhat misleading, because money launderers can exploit land frontiers by seeking protection behind them as well as create new market opportunities (Williams & Baudin-O’Hayon:129).

---

10 [http://www.unodc.org/unodc/money_laundering.html](http://www.unodc.org/unodc/money_laundering.html)
3.1.1 Traditional Money Laundering
The mode of money laundering can be described as a dynamic three stage process including placement, layering and integration. The placement stage is the initial entry of the funds into the financial system moving it away from direct association with the crime involved. This can be accomplished by depositing the money in domestic financial institutions. If the country of crime commitment is subject to strict financial regulation, an alternative is smuggling the money abroad and deposit it in less regulated jurisdictions. Another layering technique is buying up high value goods, like artworks, noble metal and antiques which can be resold by cheque or bank transfer payment (Public Safety and Emergency Preparedness Canada, 1998). The placement stage is when launderers are most vulnerable because regularly dealing with large sums of cash increases the risks of raising suspicion. To reduce this vulnerability dirty money can be legitimized through fictive loaning bills from unknown shell companies, or brass plate companies, which are fictive companies having no assets or operations of its own but are used by their owner to conduct business dealings\(^\text{11}\). The second and most complex step of the process is the layering stage which takes place through a series of transactions designed to hide the origins of the funds. This is where the global dimension of money laundering appears. Funds are sent electronically from one country to another, and are subsequently spilt up into investments in advanced financial options or in overseas markets, being constantly relocated to evade detection. The money trail can also wriggle along between shell companies. At this stage faith is put in weak legislation and delays in juridical or police cooperation. As the money goes deeper into the international financial system it gets more difficult to identify its origins. Finally, at the integration stage a perception of legitimacy is created for the money to make it available to the criminal again. For smaller amounts this may be achieved by making withdrawals on secure credit cards issued by banks in financial havens. For bigger amounts it can be obtained by creating forged capital gains, for instance by

establishing commercial businesses structured in a way where a shell company takes the loss and a home company benefits (Blum et al. 1998:19). Figure 1 illustrates the three laundering stages.

![Figure 1-The laundry cycle](http://www.unodc.org/unodc/en/money_laundering_cycle.html)

Not all money laundering typologies are this sophisticated. The simplest form is buying up race horse betting slips at racetracks, a technique combining all three stages in one operation. The real winner is paid above the original winnings in return for a legitimate receipt for the illegally obtained funds; however, this is not a reasonable technique to pursue when dealing with large sums on a regular basis. In these situations launderers may establish legal cash based businesses like retail shops and restaurants, where legal and illegal money is mixed, making the business appear more successful than it is (Blum et al. 1998:13, Gilmore 1999:36).

### 3.1.2 Modern Laundering Trends

Stricter regulation of financial institutions during the last decades has conjured money launderers’ dependence on bribing banking officials to avoid law enforcement suspicion. But
increased focus on the risks involved if getting entangled in laundering scandals has forced criminals to seek other techniques, and today’s financial system offers a wide range of instruments available. The financial infrastructure can be said to have evolved into a global system of money in the form of digital symbols on computer screens, referred to as “megabyte money” (Williams & Baudin O’Hayon 2002:132). Financial innovations in ICTs offer the benefits of speed, distance, anonymity and minimal audit trail amid daily fund transfers (Gilmore 1999:33).

The financial system allows electronic value to be represented digitally by electronic patterns. This does in effect not represent something new since it has been used by financial institutions for a long time. But technological advances including rapid networked communications with low costs per transaction, improved computer technology and mass production of chip cards and powerful public domain cryptography, have triggered widespread use of electronic cash (the Public Safety and Emergency Preparedness Canada, 1998). This can be transferred over the internet or through smart cards. The internet, “a ‘network of networks’ linking regional networks through a common communications protocol or language” (Molander et al. 1998b:7) constitutes the core of electronic commerce. Limited to academic and military research from its introduction in 1969, in the 1990s internet usage started spreading at accelerating speed and became an omnipresent interactive source of communication in the global marketplace (Dicken 1998, Molander et al.1998b). A smart card is embedded with a microprocessor and/or a memory chip. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory chip card (for example pre-paid phone cards) only can undertake predefined operations. A myriad of smart card categories are developed to enhance financial services, and are evolving rapidly into new market applications. Smart cards, also labelled stored value cards, contain money and have a built in cryptography which secures digital identity. They are different from magnetic stripe
cards in the sense that they offer greater memory storage as well as data security and processing. All functions and information are carried on the card; therefore they do not require access to intermediaries in the conduct of transactions.  

The introduction of these payment technologies affects the lives of ordinary people by providing them with the benefits of reduced transaction costs and increased efficiency of payment methods (Molander et al 1998b:1). Known under a collective term as cyberpayments, the common denominator of these technologies is that they support electronic transfer of value (Molander et al. 1998a:1). The reverse of the medal however, is the vulnerability of these payment methods to exploitation by money launderers. As stated by Molander et al. (1998a:16), “Cyberpayment systems have the potential to eliminate the money launderer’s biggest problem, the physical movement of large amounts of cash”. Moreover, Blum et al.(1998:28) argue that electronic payment systems in many ways represents a launderer’s dream since they offer the opportunity to imitate the patterns of legitimate transactions. Designed to imitate paper money in the sense that it passes immediately between two transacting on-line parties, is independent of intermediaries and leaves no audit trail, cyberpayments leave financial and law enforcement officials with obstacles to detection because the principle of knowing-your-customer is depreciated. This “disintermediation” in turn allows money launderers to avoid traditional law enforcement methods because anonymity is secured. Anonymity in combination with the speed of wire transfers and a wide variety of cyberpayment service providers moreover allows launderers to avoid credit card denomination limits and expiry dates, by holding multiple credit cards, multiple card holders and employing multiple card issuers. These payment technologies enable criminals to exploit national differences concerning security standards and rules regulating illicit financial activity.

(Molander et al. 1998a:16), and conceal the movement of illicit proceeds. Figure 2 illustrates how money laundering can take place by the use of smart cards and communication technologies.

By applying this example on the initial stage of money laundering, placement can be achieved by using a smart card or a personal computer (PC) to deposit money into an unregulated financial institution. Drug money can be invested in smart cards that are denominated in a certain value equivalent to the price of the drugs. The cards are then brought to a retail store where a merchant, who in return for a standard fee, uploads the electronic value on the card to an account in a financial institution. Once this stage is accomplished, layering and integration can be normally conducted in ways referred to in section 3.1.1. Layering and integration can also be conducted without the involvement of an intermediary financial institution through a PC instantaneously sending the funds through different layers over a network emancipated from national borders (Public Safety and Emergency Preparedness Canada, 1998), for instance as payment for internet services. At costs limited to web area rental large amounts of money can be laundered by establishing payment services like internet gambling or porn sites.
Sales are provided for by using the service and paying for it with smart cards that are connected to an unregulated financial institution account. As the launderer is the wirepuller of the business, the money is given the appearance of legal profit from the internet service. Internet payment services establishment does not require identification of the persons initiating it, allowing the establisher to use false identity or anonymous internet connection\textsuperscript{13}. Internet banking and payment services thus make computers and smart cards a tool for transfer of dirty money, and it is difficult to control this network. Cyberpayments may therefore be labeled new laundering havens, in which private persons, firms, banks and other regulated and unregulated financial institutions depending on the network become part of the game, as victims or actors, intended or unintended.

### 3.2 A Complex Phenomenon

The factors underlying money laundering expansion must be understood in elucidation of complex and interrelated causalities and constitute too many aspects for there to be room for it in this thesis. Blum et al. have identified features of the international financial system complicating the “finding, freezing and forfeiting” of criminally derived funds. These include the “dollarization” of the black markets denominating an extensive use of US dollars in criminal business reducing transaction costs, a general trend towards financial deregulation, and a heavy proliferation of financial havens (Blum et al. 1998:22). The globalisation of modern communications and technical developments in banking and payment arrangements is claimed to have emerged in the absence of corresponding globalisation of legal frameworks, consequently offering an easy entry point of illicit assets into the financial system (Eide 1994:108, Solongo 2001:1). This view is shared by Joly who points to the development of a global financial system superior to national laws (Joly 2002:174), and that unintentionally, liberalization of the markets has triggered the emergence of parallel criminal networks (175).

\textsuperscript{13}http://program.forskningsradet.no/oekrim/bakgrunn.html
Although a complex phenomenon, a set of key factors frequently referred to as facilitators of money laundering are financial liberalization, financial havens and advances in Information and Communication Technologies (ICTs). To understand the spread of money laundering, these factors must be seen as interrelated.

3.2.1 Globalisation and Financial Liberalization

It is often expressed that globalisation has caused change for the worse. This has also been the case in relation to the impacts of financial crimes upon society, which is an oversimplification of reality. As does the statement of Mr. Pino Arlacchi at the introduction of this chapter, such views point in the direction of determinism. The globalisation concept, of which perceptions range from extreme hyperglobalist views referring to a new era and an autonomous global market, to a moderate interpretation claiming that globalisation does in fact not represent much new (Held et al.1999: 3-7), is complex. It is however commonly accepted that the world’s financial markets are radically changed, as can be illustrated by the speed and scope of money in circulation, and a position in between these contrasting perceptions of globalisation is the transformation perspective. Acknowledging great change in many areas, this notion of globalisation, which is the context in which money laundering is understood here, maintains that nor is globalisation an irreversible process, nor can it be understood neglecting the importance of social factors influencing these processes (7).

Despite the somewhat hyperglobalist insinuation of Mr. Arlacchi’s statement, a certain degree of truth lies in it. Two policy decisions were made by advanced industrialized countries in the 1950s that were important to the globalisation process; granting more freedom to market operators through liberalization initiatives and refraining from imposing effective controls on capital movements (Helleiner 1994:8). As such, financial liberalization has supported easy cross-border capital flow expansion which in turn has allowed for a flourishing of illicit transactions, thus money has been given new mobility increasing the
opportunities for money launderers to benefit from illegally gained funds (1999:2). Although not entirely global in terms of inclusion, financial liberalization is characterized by a growth in multinational banking, international money markets and cross-border listing of firms in several stock markets (Narula 2003:19). The speed of advances in financial ICTs allows for money to be relocated between fictive firms, banks and bank accounts in the time it takes to press a few computer keys. As a result the current international financial system faces difficulties in dealing with “the relatively chaotic financial consequences of global financial markets” (20). Blum et al. (1998:3) claim that “fuelled by advances in technology and communications, the financial infrastructure has developed into a perpetually operating global system in which megabyte money…can move anywhere in the world with speed and ease”.

3.2.2 Financial Havens – from Juridical Loopholes to Financial Black Holes

Proliferation of financial havens is identified as an important contributor and a necessary complement to the facilitation of money laundering (Blum et al. 1998:3). While AML professionals seek to promote transparency by enacting laws prohibiting financial secrecy, financial havens hamper this goal. Blum et al. explain why:

Once the corporation is set up in the offshore jurisdiction, a bank deposit is then made in the haven country in the name of that offshore company, particularly one whose owner’s identity is protected by corporate secrecy laws. Thus, between the law enforcement authorities and the launderer, there is one level of bank secrecy, one level of corporate secrecy and possibly the additional protection of client-attorney privilege if a lawyer in the corporate secrecy haven has been designated to establish and run the company (Blum et al. 1998:17).

This prevents governments from tracing dirty money. The investigation process in financial abuses is complex, requiring thoroughfares of numerous bank transactions, but gets additionally complicated when the money trail leaves domestic territory and relies on the willingness of foreign countries and territories to share information. The extensiveness of jurisdictions with underregulated banking systems in combination with strict secrecy policies
of financial havens is therefore likely to put an end to inquiry. The term “financial haven” is used deliberately as opposed to tax havens, which is too narrow, describing political strategies presented by politically autonomous units aiming at attracting foreign capital (Haslerud 2003:20), and offshore financial centres (OFC), which is an imprecise term referring to various phenomena including export processing zones, international banking facilities and flags of convenience (17). Financial havens comprise countries, states, colonies, cities and geographical zones where finance centres offer tax regulations that are either lax or absent and a policy of more or less strict secrecy. The crucial point is that financial havens operate with secrecy strategies hiding customer identity and are partly reluctant to cooperate in terms of international information sharing (Tranøy 2003:8). This leads to a lack of transparency owing to insufficient reporting requirements and a lack of transaction supervision, due to both a willingness to cooperate and resources available.

Financial havens were originally used by wealthy people exploiting tax loopholes in national legislation. The activity was insignificant and the number of havens, including the British Isles, Switzerland, Luxembourg and Lichtenstein, was limited (Haslerud 2003:55). Today, the number of financial havens has expanded to all continents and their growth in firms, banks and other financial institutions is often outnumbering the local population. By offering tools designed to attract foreign business financial havens can be seen as political parasites seeking to “achieve self-enrichment in ways that are detrimental to global welfare” (Tranøy 2003:4). As such, these havens can be characterized as sanctuaries for the tax payers of other countries, undermining these countries’ sovereignty by giving shelter to those having something to hide from their national authorities (ibid).

3.2.3 The Dual Role and Social Embedding of ICTs

It is hardly necessary to call attention to the position of ICTs in our everyday-life, and the financial sector is only one field in which society has come to rely on these technologies.
Questions sought answered by STS scholars are how social and technological factors interact, and a central approach within the STS studies is the SCOT theory offering an explanation of this relationship. It stresses how people are involved in the creation as well as application of new technology, which is in fact not new but modifications of existing technologies (Wyatt 1998:18), and refers to physical objects as well as human activities and people’s know-how to design and use it (MacKenzie & Wajcman 1992:3). According to Wyatt (1998) one of the features of technologies forming a legitimate basis for seeing them as socially constructed is that they represent the material embodiment of values and interests of a social group. The internet is a good example. Originally designed for military purposes, users saw opportunities for extended utility areas and improvements were designed based on these users’ needs. Likewise, electronic payment technologies were designed to reduce transaction costs and increase user-friendliness, but turned out to be vulnerable to exploitation by criminals. In turn, social needs represented by a desire to fight money laundering have formed the basis for pushing through technical countermeasures based on financial sector technologies. According to Porter (2003:537) the global financial infrastructure has evolved into a complex system of technical linkages, including electronic links between exchanges, electronic transfer systems, information networks, clearing houses and internet connections. This system can be used both for the purpose of conducting and countering money laundering. The rationale behind arguing that ICTs facilitate money laundering is that money can be moved anywhere in no time and at the same time evade law enforcement. Therefore modern ICTs represented by electronic payment systems have accelerated the laundering process. Simultaneously however, at the same time as these technologies offer both arena and hiding place for money laundering operations, they can be used to curtail the problem. When treated as a source of information gathering by law enforcement and payment system regulators, the technologies underlying
electronic payment systems constitute an indispensable tool for fighting money laundering (Molander et al. 1998a:11). This is exactly what has been the case in international AML.

3.3 Major Movers of Money Laundering Countermeasures

Targeting money laundering has entered the agenda of several international organizations and is incorporated within the legal frameworks of an increasing number of countries, which bears witness to the high priority given to breaking the money laundering chain. There are still areas of the world that are not regulated, but it can be argued that the fight against the phenomenon is starting to reach global expansion. In the following, focus is directed at important achievements of major international bodies combating the phenomenon. Considering its status as a standardizing AML body, the role of the FATF is emphasized. Under its guidance, AML developments have followed a two-track approach grounded in the 1988 Vienna Convention concerning strengthening of the criminal law and the Basle Committee Statement of Principles regarding the preventing role of the financial system (Castle & Broomhall 1998:6).

The FATF has outlined procedures to assist the implementation of international AML standards, and these procedures are conducted by using electronic payment systems as a source of information. Based on “normal” financial transactions, suspicious activities possibly prior to terrorist financing are sought identified and transaction data is stored for possible subsequent investigation. This illustrates how ICTs, or more precisely technologies underlying payment systems, can be used to combat money laundering.

3.3.1 Initiating Landmarks

The UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances adopted in Vienna in December 1988 represented the initializing stage of international money laundering countermeasures. Designated to combat the laundering of proceeds from drug trafficking, the signatories of the convention agreed to criminalize the act of money laundering and increase international cooperation, as well as to pass laws to facilitate tracing.
seizing and confiscation (Castle & Broomhall 1998:6-7). A crucial implication of the Convention was the imposed obligation to offer far-reaching mutual legal assistance by abandoning the traditional paragraph of banking secrecy (ibid).

To meet the problem of extensive use of financial institutions in money laundering schemes, the Basle Committee on Banking Supervision issued its *Statement of Principles on the prevention of criminal use of the banking system for the purpose of money laundering* in December 1988 (Castle & Broomhall 1998:6). Housed by the Bank for International Settlements (BIS), the Basle Committee consists of representatives from the central banks and supervisory authorities of the G10 group of industrialized countries. The Statement was drafted by United States representatives and seeks to encourage preventive regulation of the banking sector through adopting policies of customer identification, suspicious transaction avoidance and transaction record keeping. In conformity with the Vienna Convention the Statement requests cooperation with law enforcement authorities, although in accordance with national confidentiality regulations (8-9).

### 3.3.2 The Financial Action Task Force

The FATF is the international body in charge of protecting the global financial system against money laundering and terrorist financing. It is an independent intergovernmental body whose primary goal is to yield the political will necessary for bringing about national legislative and regulatory reform to detect and confiscate laundered proceeds and replace financial secrecy with transparency. The role of the FATF is threefold. It oversees the building of effective AML systems in its member countries, reviews laundering techniques and promotes expansion of international AML by encouraging implementation of money laundering countermeasures in non-member countries (Williams & Baudin-O’Hayon 2002:137). It has no defined constitution and no unlimited lifespan. It was set up by the G7 at the Paris Economic Summit in 1989 and has up to date been an ad hoc arrangement with a temporary lifespan.
whose mandate has been prolonged on a four year basis (Gilmore 1999:80-82), until 2004 when its mandate was expanded by eight years. There are currently 33 FATF member countries and jurisdictions and its secretariat is housed by the OECD. Presidency rotates on a one year basis and its working structure is built around multidisciplinary groups represented by national delegations. The decision-making process is based on consensus. During three annual plenary meetings policy directions and initiatives are discussed and decisions are made on the basis of papers prepared by the Secretariat or reports from delegations. The normative core of the FATF is the 40 Recommendations, set out to encourage implementation of the contents of the Vienna Convention and the Basle Committee Principles. They were first launched in 1990 and revised in 1996 and 2003 as to keep pace with laundering techniques and foresee future challenges. The 2003 version also attacks terrorist financing as formulated by the Eight Special Recommendations. Revisions are based on experiences of its member countries and on policies of other AML organizations but are open to non-members, observers, financial sector institutions and other parties affected by money laundering (Castle & Broomhall: 1998:12). The 40 Recommendations represent an international AML standard designed for universal application (Tranøy 2002:13). They are not prescriptive, but set out principles for action for their implementation to be adjusted to the constitutional structure of each country. Today’s revised version, which has been endorsed by more than 130 countries and jurisdictions, covers a broad set of bank and non-bank financial institutions and professions vulnerable to money laundering, including exchange bureaus, commodity brokers, insurance companies and money transmission services (Gilmore 1999:

14The FATF member countries and governments are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; the Russian Federation; Singapore; South Africa; Spain; Sweden; Switzerland; Turkey; United Kingdom; and the United States. The European Commission and the Gulf Co-operation Council are also members. (http://www.fatf-gafi.org).
15http://www.fatf-gafi.org/AboutFATF_en.htm#Decision-Making
17All references to the 40 Recommendations are based on the revised 2003 version.
To limit the risk of displacement to other sectors the area of application has further been expanded to accountants, lawyers, estate agents and any business accepting large cash amounts, like car dealers, auction houses, art galleries and jewellers. Briefly summarized the message of the 40 Recommendations is to:

- Criminalize money laundering and enact laws to confiscate proceeds of crime
- Maintain rules for customer identification and record-keeping in financial institutions, and pay special attention to new technologies favouring anonymity
- Require reporting of suspicious transactions to authorities
- Keep adequate systems for control and supervision of financial institutions
- Make the preconditions necessary to contribute to effective international cooperation at all levels

A closer explanation can be provided to some of the above points. Customer identification rules intend to prohibit anonymous customer relations. The purpose of record-keeping is to make transaction information available to authorities for backtracking in relation to investigations. A piece of information might not be relevant to law enforcement at the time of registration, but if prosecution attached to a person linked to the transaction is initiated later, this information can be crucial, thus transaction records are required to be kept for five years. The rationale behind paying attention to new technologies is that despite the admitted lack of evidence of cyberlaundering at the time of inclusion of this request (Recommendation 8), these technologies were seen as potential obstacles to effective AML (Gilmore 1999:93). Paying attention to suspicious transactions can be an awkward task due to troubles of determining what is meant by it. A common yardstick is the imposed limit to transactions above a certain amount (USD 10.000), but this has been evaded by money launderers through “smurfing”; the structuring of transactions right below reporting limits (31). What also

---

19 The EU was in fact the first body to introduce rules concerning the inclusion of lawyers and accountants in relation to reporting requirements. This forms part of the second EU Directive. The FATF included these professions later (Information retrieved from interview with an AML professional, June 2004)
renders this task difficult is a lack of proximity to visible money laundering victims. Affecting the community in general, a position of not-in-my-term-of-office is easily adopted. This leads to an open-handed follow-up of reporting requirements by banking officials, allowing criminals to seize a bigger share of societal goods, offering less to others (Eide 1994:109).

Implementation of the 40 Recommendations can be ensured through a set of mechanisms ranging from relatively modest persuasion to more coercive instruments. At the one extreme lies technical assistance provided by FATF experts from legal, financial and law enforcements fields to identify areas of improvement and backwardness and offer compliance guidelines to those seeking to meet AML standards. Apart from receiving advice in establishing legislation, governments have been encouraged to train financial sector personnel and set up Financial Intelligence Units (FIUs) to monitor transactions (Williams & Baudin-O’Hayon 2002:137). These FIUs analyse and process reports on transaction activity and arrange for rapid exchange of information between financial institutions and law enforcement authorities as to facilitate detection of money laundering. As part of the technical assistance strategy, a detailed methodology based on the 40 Recommendations and the 8 special Recommendations to evaluate AML and anti-terrorist financing efforts has been agreed upon in collaboration between the FATF, the IMF and the World Bank. Further, mechanisms of mutual evaluation and self-assessment exercises are conducted through which each member country provides status information by responding to a questionnaire. This information culminates in annual typologies exercises drawing on recent potential obstacles to effective AML, like wire transfers, cyberpayments, shell companies and shell individuals, politically exposed persons (PEPs), gate keepers\textsuperscript{20}, terrorist financing, non-bank financial institutions and non-financial professions vulnerable to money laundering (Gilmore 1999:101). These mechanisms serve as

\textsuperscript{20} Politically exposed persons refer to “individuals who are or have been in the past entrusted with prominent public functions in a particular country” (FATF Typologies 2003-2004:19). Gatekeepers here refers to the involvement of various legal and financial experts from whom money launderers seek advice or services (FATF Typologies 2003-2004:24).
peer group pressure in which responsibility is laid in the hands of the member countries for them to actively work towards compliance. Moreover, there are monitoring mechanisms to ensure that all participants have adequate supervisors with the power to secure compliance as well as authorities to review effectiveness of the actions taken. Finally, coercive means of sanctioning or threats of sanctioning can be found at the other extreme. For instance, in 2000 the FATF compiled a list of non-cooperative countries and territories (NCCTs), a dynamic naming and shaming process based on the degree of compliance with the 40 Recommendations. Fifteen jurisdictions were initially listed and these countries would remain listed until their policies were improved. As of July 2004 there were six NCCTs left\textsuperscript{21}.

The putting into practice of the 40 Recommendations illustrates how the same technologies potentially exploitable to money laundering can be used as an instrument to curtail it; the requirements of suspicious activity reporting and record-keeping and the subsequent possibility of backtracking relevant information are based on transaction data. Cracking down financial haven secrecy has been among the top priorities of the FATF. Apart from the naming and shaming process, discussions have been initiated with the Society for Worldwide Interbank Financial Telecommunications (SWIFT)\textsuperscript{22} in order to prevent customer anonymity when dealing with customer transfers (Gilmore 1999:102). International community pressure has subsequently forced many financial havens to cooperate with foreign governments.

As part of an overall objective of spreading the AML message the FATF has encouraged creation of several regional style bodies to follow up on mutual evaluations and reviewing

\textsuperscript{21} The initial NCCTs were the Bahamas, Cayman Islands, Cook Islands, Dominica, Israel, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Panama, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines. The 6 remaining NCCTs are the Cook Islands, Indonesia, Myanmar, Nauru, Nigeria and the Philippines. (http://www.fatf-gafi.org/NCCT_en.htm).

\textsuperscript{22} The SWIFT is a worldwide community through which financial institutions connect to one another, whose purpose is to be the leader in communications solutions enabling interoperability between its members, their market infrastructures and their end-user communities, http://www.swift.com/index.cfm?item_id=41756
new laundering trends in their respective areas\textsuperscript{23}. Increasingly, larger areas of the world are being covered by money laundering countermeasures, aiming at securing an impermeable AML network. In addition to these regional bodies, the FATF also cooperates with other international bodies and organizations. FATF principles have been implemented within the frameworks of the EU, the European Council and the UN inter alia, although these bodies also have developed independent AML policies. In particular, the UNODC launched an important AML research programme, the Global Programme against Money Laundering (GPML) in 1998, which offers an extensive technical assistance programme\textsuperscript{24}.

\textbf{3.3.3 Law Enforcement Engagement: the Egmont Group}

The problem arising when money trails leave domestic territory explains why enforcement authorities have endeavoured to establish mutual international information sharing. Interpol is the largest formal international police organization facilitating cross-border law enforcement cooperation (Gilmore 1999:69). It offers a global communication system based on wide-reaching criminal databases and analytical services\textsuperscript{25}; however, money laundering forms but part of its agenda. An international grouping that focuses specifically on money laundering is the Egmont Group, currently consisting of 94 countries. Opposed to Interpol, the Egmont Group has an informal mandate. Arising out of a Belgian/USA initiative, it came into being in 1995 as a FIU network (72). Due to the inertia of countries' traditional law enforcement systems, obligations on mutual information sharing was an underlying motive for the FATF to encourage creation of FIUs (Recommendation 13 and 14). Accordingly, the cornerstone of this grouping is the availability of financial information to national authorities stored on an encrypted web page. It permits members to “access information on FIUs, money laundering

\textsuperscript{23} These regional bodies comprise the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL, former Council of Europe PC-R-EV), the Financial Action Task Force on Money Laundering in South America (GAFISUD), the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), and the forthcoming Middle East and Northern Africa regional body.


\textsuperscript{25} http://www.interpol.int/Public/Icpo/default.asp
trends, financial analytical tools, and technological developments” (Gilmore 1999:73). To obtain a joint international understanding of laundering techniques, the Egmont network practises modes on recent lines of action and uses the network to inquire about members countries’ experiences. The Egmont collaboration network thus represents something new regarding law enforcement working methods in trying to operate ahead of criminals rather than always lagging behind. It is a response to a modern crime picture requiring corresponding modes of countermeasures.

3.3.4 Financial Sector Engagement: the Basle Committee and the Wolfsberg Group

Millions of wire transactions a day leave law enforcement officials to rely on banks, insurers, exchange bureaus and other financial intermediaries to unveil illicit transaction activity. The recognition that financial institutions are being used in money laundering schemes has triggered financial sector engagement. Potential implications of getting involved in laundering scandals have encouraged a focus on public confidence and credibility maintenance, as to avoid negative publicity severely affecting the business. Adopting the contents of the 1988 Basle Committee Principles can contribute to avoid such situations. Moreover, the 1997 Basle Committee Core Principles for Effective Banking Supervision encourages banking supervisors to make sure their banks have adequate preventive policies, which is ensured by building supervisory capabilities of central banks and other financial intermediaries²⁶.

Pieth and Aiolfi (2003:2) claim that “in 1988 it was the banks themselves that requested the movers of the G7 countries and others to clamp down on illegal drug markets”. When AML instruments were imposed on the banking world in the 1990s however, many banking institutions were unprepared because customer identification and reporting requirements represented something new and controversial to many countries. It led to uneven implementation which in turn left banking institutions with perceptions of a tension between

²⁶ http://www.bis.org/publ/bcbsc102.pdf.
the costs of AML and the benefits of containing financial crimes, as well as the risk of losing customers to competitors offering weaker regulation. Thus an emerging “patchwork of rather diverse rules” cleared the way for money launderers to exploit these incongruities (Pieth and Aiolfi 2003:3). Harmonization of divergent AML regulations was needed and this initiative came from the banking sector itself. As an association of twelve global banks aiming to develop financial services AML and terrorist financing standards, the Wolfsberg Group came together in 2000 to draft private banking guidelines known as the Wolfsberg Anti-Money Laundering Principles for Private Banking27 (4). Like the Basle Principles, the Wolfsberg Principles seek to prevent use of the banking system for money laundering purposes. Because of its late arrival, it has been criticized for not representing anything new, in addition to being a voluntary code of conduct not likely to bring along significant results. However, as stressed by Pieth and Aiolfi the strength of the principles is found in the commitment of participating banks to ensure compliance in all their operations, including offshore centres. What makes the Wolfsberg Process special despite its criticism is that it represents an independent private sector contribution to fight money laundering and it is built on a risk based rather that a rule based government approach, which will be further discussed in the analysis. Accordingly, the Wolfsberg Principles specifically help banks determine the degree to which they should engage with AML requirements.

3.3.5 Fresh arrivals: the IMF and the World Bank
As revealed above, concerted action has been taken by many important international bodies and organizations to combat money laundering. Similar engagement from the IMF and the World Bank has been much awaited by the international community. The FATF naming and shaming strategy turned out to be efficient in terms of targeting non-compliant actors; however, in 2003 it was abandoned and replaced by a more consensual and inclusive audit of

27 http://www.wolfsberg-principles.com/
offshore jurisdictions under direction of the IMF (Sharman 2004:22). The IMF audits are only published by approved of each jurisdiction. Rather than receiving a distinction as compliant or not, the jurisdictions in question can make comments to the report (ibid). In the period between 2002 and 2003 the IMF and the World Bank conducted a twelve month pilot program assessment of international standards in both industrialized and developing countries, in cooperation with international colleagues. Since then, the IMF has received requests from more than 100 countries to help establish AML frameworks. As from March 2004 the boards of the Bank and the Fund finally agreed to take on comprehensive action by conducting compliance assessments with international standards in their member countries and offering country-specific technical assistance to those in need of it. In cooperation with the FATF, the two institutions have arranged workshops for regional bodies and developed a methodology for assessing compliance with the 40 Recommendations. The annexation of these bodies indicates an AML framework which is about to reach global expansion.

### 3.3.6 Electronic AML

An attempt to improve efficiency regarding money laundering detection is not far away. As the first country in the world, Norway has passed a law requiring all financial institutions to introduce electronic monitoring solutions by 2005. This puts responsibility in the hands of financial institutions. These solutions are built on USA models and include risk based scenario modelling of customer activity based on networked financial institution data which, by employing linkage analysis, enables the tracking of unusual patterns. It is crucial that this modelling is not predefined but based on covariance analysis in which input data changes over time. If a customer suddenly changes behaviour for instance, and uses a bank known for laundering money, the system posts an alert for the situation to be investigated. Top-tier brokerage firms such as the British Morgan Stanley and Unity Trust Bank, and Bank of

---

28 Interview with an AML professional, June 2004.
America have taken a lead in implementing and testing this technology, in which the goal is to risk-rank unusual transaction activity but also guarantee accuracy by minimizing false alarms. Electronic AML technology is not primarily set out to detect money laundering, but to help financial institutions comply with regulations. These solutions also safeguard financial institutions through knowing-your-employee. The system reveals who conducts transactions and stores patterns of employee activity, and can to some extent meet the problem of corruption. Expected outcomes of this process are significant increases in suspicious activity reports, and consequently increased exposure of money laundering cases. This can however only be achieved in so far as the working procedures within financial institutions are followed up in conformity with the technological solution. Especially important is the process of examining alerts to determine if there is reason for further investigation. In doing so, financial institution officials are authorized to abandon professional secrecy, therefore reporting must be reasonable. This reveals that combating money laundering does not solely depend on regulative and technical efforts, but on human resources, indicating that AML technologies are socially embedded. Electronic AML is still at its elementary stage and is not meant to replace manual reporting systems but to complement them by intercepting complex connections that are impossible to trace manually.

A Norwegian initiative meeting the problem arising when money leaves domestic territory is the Norwegian Currency Register, entering into force in 2005. As an improvement of previous constellations, it seeks to control funds flows in and out of the country and imposes duties for banking institutions to report all incoming and outgoing transactions including cash and credit card transfers above a certain amount. The register makes information directly accessible to law enforcement authorities.

***
Having demonstrated how payment technologies can be used both to support and counter money laundering, and having presented major contributors to international AML, attention can now be directed at deciding if there exists an international regime in this issue area. The dependence on technologies in fighting the phenomenon gives a hint of linkages to a technological system. It can be asked if the technical features of international AML has any effect on AML policies. In the following chapter these questions will be addressed. It will also be explained why enhanced international action has been taken against the problem.


4 Explaining AML Emergence and Conduct

4.1 Introduction
Governmental interest in fighting money laundering has been an issue only since the late 1980s, but during this period international AML has gained momentum. The fact that a group of states have succeeded in initiating and conducting extensive AML efforts contradicts a common assumption in international political economy about the loss of power of states following globalisation (Helleiner 1999:2). Quite contrarily the achievements of the international AML nexus are so thoroughly coordinated that it can be asked if there exists an international regime to regulate the issue area. Continuously working towards common goals, rules and practises for regulation, law and monitoring, objectives of criminalizing money laundering and simplifying international cooperation have been reached. Section 4.2 demonstrates that international AM can be labelled an international regime. Section 4.3 describes the characteristics of international AML and demonstrates that it possesses the features of a technological system. An explanation to growing international responses to money laundering is offered in section 4.4. The effectiveness of international AML will be briefly discussed at the end of this chapter.

4.2 Identifying International AML as an International Regime
The components of the definition of international regimes can be identified within international AML. The principles component, referring to general formulations of objectives and basic understandings about how the world works, can be linked to the aims of international AML, which are to promote policies to combat money laundering by removing the proceeds from criminals and subsequently also the motivation to continue the activity. Transparency constitutes the key principle on which all financial activities should be built. The norms component describing rights and duties of states and specifying general standards for behaviour can be formulated as the right of all countries to operate within a just financial
system. Achievement of this requires all countries to contribute to international cooperation through compliance with international AML standards. To secure the underlying principle of transparency, all financial secrecy provisions must be abandoned and relationships supporting the use of anonymous shell banks and companies must be denied. In return, every country making an effort to reach compliance is entitled to technical assistance provided by leading AML bodies that are obliged to safeguard the interests and opinions of all member countries. As specific directions for behaviour at a lower level of generality than the two former components, the rules component is identified through an extensive framework of specific measures to be implemented in participating countries. These include inter alia reporting requirements of suspicious activities, record keeping requirements, policies for securing customer identity, and requirements to establish FIUs. The identified principles, norms and rules constitute the substantial part of the regime.

<table>
<thead>
<tr>
<th>Box 1. The regime components of the international AML regime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The substantial part of the AML regime:</strong></td>
</tr>
<tr>
<td><strong>Principles</strong></td>
</tr>
<tr>
<td>-Secure financial transparency</td>
</tr>
<tr>
<td>-Remove profit from criminals</td>
</tr>
<tr>
<td><strong>Norms</strong></td>
</tr>
<tr>
<td>-Comply with international AML Standards</td>
</tr>
<tr>
<td>-Abandon secrecy provisions</td>
</tr>
<tr>
<td>-Deny anonymous customer relations</td>
</tr>
<tr>
<td>-Receive technical assistance from AML bodies</td>
</tr>
<tr>
<td><strong>Rules</strong></td>
</tr>
<tr>
<td>-Suspicious activity reporting</td>
</tr>
<tr>
<td>-Customer identification requirements</td>
</tr>
<tr>
<td>-Record keeping</td>
</tr>
<tr>
<td>-International information sharing</td>
</tr>
<tr>
<td>-Establish FIUs</td>
</tr>
</tbody>
</table>

The operational part of regimes contains procedures identifying practices for implementing rules. In the context of an international AML regime, of which the contours by now should be settled, the mechanisms for ensuring implementation of the main principles of the 40
Recommendations can be recognized as such procedures. Including technical assistance, mutual evaluations and monitoring, these procedures ensure the putting into practice of the rules to be implemented in member and non-member countries. In fact, by its mandate, localization and staff, the FATF itself constitutes the operational part of the regime. International AML clearly possesses features applicable for all components of the definition of an international regime. Having determined that there is an international AML regime, it must be investigated what sort of regime this is and which of and at what stages of the process the approaches to international regimes prevail.

4.3 The Material and Social Embodiment of International AML

It has been argued that in issue areas where there exists a technological system the technical features of this system can influence the way politics in that issue area operate. To support the assumption that international AML is a technology intensive issue area attention can be directed to its initial stages. The reasoning why enhanced action was initiated against money laundering is grounded in concerns with increased drug related money laundering and a subsequent abuse of financial system instruments in money laundering schemes. To attack this problem AML requirements based on financial transactions, like suspicious activity reporting and information processing, were implemented. This gives a hint of the technical characters of international AML, but is it also a technological system? The presence of system components shows that it is. Extensive use of the financial system infrastructure in the fight against money laundering, including information processing based on electronic payment systems reveals evidence of physical artefacts. This refers to the networked machines, hardware, software and optical fibres constituting these payment technologies. The number of bodies engaged in AML, the FATF, the UN, IMF, the World Bank, financial institutions and enforcement bodies inter alia leaves little doubt to the presence of organizations. The structure of many of these bodies also gives a hint of their technical structure. A quick glance at the
FATF web pages indicates that its structure is practically oriented around the demands of the task to be solved, which can be illustrated by the annual typologies exercises. A technical focus is also central to the Basle Committee on Banking Supervision. It has no organizational chart or articles of agreement, but operates through informal subgroups and task forces based on consensus and processes of mutual education (Porter 2003:536). The Egmont network of FIUs is another example of technical informal cooperation. Modes on recent laundering techniques are practiced and the goal is to operate ahead of crime commitment. Scientific components can be exemplified by the FATF typologies and FIUs. Finally, legislative artefacts are identified in national legal policy frameworks. Examples include requirements of customer identification, suspicious activity reporting and record keeping procedures expressed by the USA Patriot Act. These system components can exist without there being a system, thus evidence of material embedding must be provided. Consistent with theory, this must be sought in the interaction between human and non-human actors. An example is the use of financial instruments in the implementation of rules and procedures, and this is particularly evident after the terrorist attacks of September 11th 2001 when international AML took on a more risk based approach. For instance, the so called dataveillance techniques; “the proactive surveillance of what effectively become suspect populations, using new technologies to identify risky groups” (de Goede 2004:7) illustrates this. It is a technique which relies on sophisticated computer technologies built on mathematic modelling and entails classification and analysis of financial transaction data which “relies on the prior construction of ‘normal financial transactions’” (ibid). These technologies allow for communication between the actors involved but are not optimal if not networked. A specific reference to such networked technologies is the SWIFT community through which financial institutions communicate.
The adopted risk based intelligence strategy based on the searching for suspicious activity indicates a watershed in international AML. Before the terrorist attacks international AML used transaction technologies to trace drug related money after crime commitment. After the terrorist attacks focus was primarily directed at preventive electronic surveillance of financial activity in order to predict terrorist financing, in which all actors basically are rendered suspects (de Goede 2004). It can be questioned if the regime has changed from an AML to an anti-terrorist financing regime; however, that would be misleading because money laundering and terrorist financing represent different needs. Money laundering involves the cleaning of dirty money as to hide the funds’ origins and is profit motivated, and terrorist financing entails a “soiling” of clean money as to hide the destination of the funds and is ideologically motivated. The new regime reflects the threat to society which had changed to “clean money intended to kill, not illicit proceeds of crime looking for a place to hide” (de Goede 2004:3). Countermeasures consequently had to reflect this new threat as previous techniques appeared inefficient, which can be illustrated by the statement of a chairman of the US National Security Council Committee on Terrorist Financing after the terrorist attacks: “Last year the promise of decades of work was silenced by the assault on New York and Washington” (ibid). What separates the AML tracing strategy from the preventive anti-terrorist strategy is that the threshold for violating civil liberties has shifted towards an increased political will to overrule civil rights. International terrorism represented as a greater immediate threat than money laundering, thus the use of more controversial means of combating the problem could be legitimized. In turn, the Patriot Act offered incentives to design and use technologies that infringe the civil liberties.

The intension behind emphasizing the contribution of a technological system in the regulation of international AML is not to depreciate the role of power, interest and knowledge based theories. But the character of contemporary international AML must be viewed in light
of the interaction between physical and human dimensions on which it is built. The AML regime includes “a constellation of (inter)national policy bodies, intelligence agencies and private actors, and encompass techniques of training, reporting and regulating” (de Goede 2004:24), and such technical arrangements can influence AML policy directions.

4.4 Explaining AML formation and persistence
This section explains why so many countries have complied with international AML standards. It will be demonstrated that the relevance of the various theoretical approaches presented in chapter two must be seen in relation to different stages of the regime process. Therefore they must be seen as complementing rather than competing. First, the contribution of the power based approach is seen in relation to the dominant position of the USA and the FATF. Second, it will be demonstrated that countries are starting to realize the benefits of collaborating against a common enemy, consistent with the interest based theory. Third, the role of expert knowledge in international AML is assessed, and the relevance of the technical authority concept will be opposed to scientific knowledge exemplary of epistemic communities. Finally, it will be demonstrated that international AML is path dependent in the sense that it is subject to the momentum acquired through its own evolution.

4.4.1 State power: the Role of the USA
It is commonly accepted that the USA in many respects is a hegemonic power. In the international AML context the USA used its power to initiate countermeasures. Evidence of this is found in the Vienna Convention and the Basle Committee Principles. Although the negotiating of these initial landmarks was conducted in cooperation with European actors, they largely set out to meet US concerns. According to the power based approach this hegemonic role of the USA would have to persist as for the regime to be maintained. Three incidents symbolize how other states yielded submission to the will of the USA. The first incident illustrates the significance of the US share of the world’s financial markets, and
supports the theoretical assumption regarding the ability to control power resources. In relation to a drug investigation in the early 1980s US governments requested access to financial information from branches in the Bahamas and the Cayman Islands. As they refused, threats of seizure of their US assets made the branches give up the information, and mutual legal assistance treaties were signed between the parties to combat money laundering (Helleiner 1999:31). Since this took place before the initiating of the Vienna Convention it does not explain US hegemony in relation to international AML, but it is likely that the episode triggered a US will to promote international cooperation. Second, in the late 1990s President Clinton initiated a proposal to strengthen AML, but it was restrained by a republican dominated congress unwilling to go through with any change limiting the courses of action in the banking sector (Pieth & Aiolfi 2003: 272). However, the Clinton administration did succeed in promoting the top-down black-listing of NCCTs. A proposal was made to three multilateral bodies to name and shame countries that had developed underregulated financial centres by 2000, and it was undertaken by the FATF, the OECD and the Financial Stability Forum (FSF)\(^3\) simultaneously (Wechsler 1998:49). In the aftermath of this process the financial ministers of the G7 threatened to restrict financial transactions with listed jurisdictions, and limited support from international financial institutions would be considered if they did not undertake efforts to adopt AML policies (50). Consequently almost all listed countries adhered to the requirements. Third, when the Bush administration entered the scene in 2001 there were government officials who were sceptical to impose stricter regulations against money laundering and financial secrecy. But the terrorist attacks of September 11\(^{th}\) 2001 gave rise to a policy u-turn as linkages were discovered between money laundering and terrorist financing. Six weeks later the Patriot Act was passed. It formed a legal basis requiring financial institutions to establish policies to tackle money laundering and terrorist

\(^3\) The FSF was formed in the wake of the Asian financial crisis to “promote international financial stability through information exchange and international co-operation in financial supervision and surveillance” (http://www.fsforum.org/home/home.html).
financing which, at a minimum, must include internal procedures, policies and controls to
guarantee for compliance officers, employee training and instituting program testing by
independent auditors in all financial institutions. The mentioned dataveillance system is a
product of the Patriot Act requirements. An example of such systems is the so-called
MATRIX (Multistate Anti-Terrorism Information eXchange). It serves as a database in the
search for irregularities and contains government files on all US residents based on personal
data collected from the government and from private companies (de Goede 2004:8). Although
with only domestic sphere of application, the Patriot Act directs the international community
in general and led to expanded commissions of the FATF and enhanced international action
against money laundering and terrorist financing. These three incidents symbolize that the
USA used its hegemonic power to make other countries adhere to their will and promote
AML development and compliance, and is in accordance with one of Krasner’s three ways in
which states can exert power on other countries. By taking such a controversial step violating
the privacy rights of US residents to combat money laundering, a desired achievement apart
from cracking down on terrorist financing may have been to win top tier status, whereas less
compliant countries would be further frowned on. Despite its range of application restricted to
domestic actors, the Patriot Act can make things difficult for foreign actors that are
economically dependent on the USA and whose AML level of ambition does not oblige to US
requirements. Due to its infringements of civil liberties the Patriot Act has been object to
sharp criticism even from FATF officials. This can and has led to precautious extradition of
information to the USA from collaborating FIUs, thus it can in this sense be said to have
defeated its own end. This illustrates that although the USA in many respects uses its
hegemonic power, it is misleading to claim that AML regime persistence exclusively can be
explained by the hegemonic role of the USA.

---

31 According to one of the interviewees, information is not provided to the USA unless it can be justified.
Contributions of international AML to an international regime basically centre on the work of the FATF. Consistent with the expected findings, Krasner’s remaining two ways in which countries can exert power; regarding who decides who may participate in the game and who prepares policy frameworks, are maintained by the task force. Although new members have been added since its initiation, it is not an accidental ensemble of countries that has been invited to join the forum. There are countries interested in becoming members that are not welcomed; however, universal adherence to international standards is encouraged. As a forum put together by the G7 it was natural that these countries decided who should be invited to participate. These countries’ influence can be justified because they contribute largely to the financing of AML cooperation, which is also justified since the positioning of these countries as core industrialized states and major financial centres suggests that they are the largest beneficiaries of collaborated AML.\textsuperscript{32}

The task force also holds the power to arrange AML policies. It has provided design of the regime, regime contents and objectives formulated by its recommendations, and outlined guidelines for administering the putting into practice of AML policies. FATF guidelines have also been implemented within the frameworks of cooperating bodies and organizations such as the EU and the UN. The procedures for ensuring compliance with FATF directions for behaviour are internationally agreed upon and are followed up by member and non-member countries, and this effecting of its recommendations despite its lack of executive power bears witness to the role of the forum as the chief executive of international AML. But keeping in mind that it is an international body consisting of many member countries holding different views on how things should be conducted, the question must be asked which countries within the FATF are most directive. The forum is backed by each member’s government and is as

\textsuperscript{32} The sums passing through these countries and the expected extensiveness of money laundering within these nations naturally explains why these countries are particularly eager to overcome the problem.
already mentioned not an accidental composition of countries. Certainly, the decision making process is based on consensus, and members are evaluating each other on a regular basis, but its mandate thoroughly reflects the desires of the most influential actor. The 2000 blacklisting process illustrates this. But it also reflects the power constellations between the most powerful actors within the task force. When preparing the NCCT list Britain wanted to include Switzerland due to their financial secrecy provisions. Switzerland responded by claiming to make sure Britain was black listed if they were. Accordingly, a compromise between the two was entered into in which they agreed that both would remain off the list (Sharman, 2004:7). Moreover, the USA has been criticized by Germany for not meeting the requirements of knowing-your-customer. Although a US Senator admitted that Delaware had less compliant standards than some of the listed NCCTs, the German protest was clamped down and it was unthinkable that the USA should end up on the list (ibid). This is just another example supporting the argument that US hegemony is crucial in securing regime maintenance, although it can not be ascribed exclusively to the USA.

4.4.2 The Benefits of Cooperation
Despite the criticism of top-down policy strategies, maybe the use of power has served as a precursor both to establish a solid framework and create incentives for recognizing the benefits of cooperation. A desire to identify with highly compliant countries in order to gain acceptance from the international community offers incentives to adopt far-reaching AML policies. As one of the greatest fears of banking and other serious financial institutions is to obtain reputations for doing business with criminals, investing in AML is crucial. In comparison, the risk of being fined for not taking action seems trifling since these costs are minimal opposed to the expenditures of losing customers and business integrity. The fear of getting entangled in money laundering schemes therefore serves as a strait jacket, but may also be a threshold for reporting offences. Since financial business primarily is profit
motivated, and because this motive depends on customer confidence, an assessment must be conducted to estimate the costs of reporting the offence versus keeping quiet about it. But anyone choosing this strategy is faced with the risk of being charged with non-compliance. In turn, countries and jurisdictions that are housing non-compliant actors risk repercussions like restricted access to markets, as illustrated by the strategies conducted by the USA. As such AML is by many countries perceived as an unjust top-down policy. Increasingly however, as a growing number of laundering scandals and their effects have reached the headlines of international news magazines, optimistic attitudes towards compliance have been reinforced, and AML bodies are receiving positive feedback from countries and financial institutions having admitted the advantages of compliance. The explanation to this is not found in a will to contribute to catch other countries’ crime perpetrators. Rather, next to the fear of losing respectability a growing number of countries realize the benefits of receiving assistance in catching their own bad guys. Countries suspecting that their financial institutions are extensively used in money laundering schemes have a self-interest in international cooperation in order to overcome their dilemma. Thus, common AML mechanisms, for instance international information sharing, may contribute to detect money laundering operations. This may be related to states’ self-interest in bringing back lost income kept in financial havens, a view rooted in the assumption that commercial motives are omnipresent. Countries fear competitive deregulation and a subsequent loss of mobile finance capital to foreign markets (Helleiner 1999:28). Governing a state is thus equated with running a business: loss of income requires countermeasures. Besides, vast sums of money kept in financial havens reduce the possibilities to maintain substantial social welfare systems.

Rather than reflecting countries’ profit motives, international AML must be seen as a response to a changing criminality picture. Enhanced international engagement with AML

---

33 This is the impression I was left with after having analyzed the interviews.
goes back to the 1980s and growing concerns with increased organized profit motivated crimes. At the 1989 Paris Summit, the G7 stressed the “urgent need for decisive action, both on a national and international basis to counter drug production, consumption and trafficking as well as laundering of its proceeds” (Gilmore 1999:79). Partly the AML campaign seeks to remove unfair competitive advantages for those conducting illegal business and to prevent criminals from obtaining influence in the financial system. Because money laundering is a cross-border activity countermeasures naturally have to be as impermeable as possible to avoid loopholes. The nucleus of the problem relates to enforcement authorities’ recognition that profits were not removed from criminals although they were sentenced. Traditional investigation and prosecution techniques were built on reactive methods requiring crime reporting before action could take place. Since this seemingly this did not succeed in making the crime less beneficial, these means for fighting profit motivated crimes were insufficient. Efficient crime combating subsequently needed to be rooted in proactive techniques based on financial investigation. This is a different way of thinking where legal offences are unveiled by receiving tips on suspicious activity. Intentionally, this will in turn contribute to remove the proceeds from criminals and consequently also their motivation to continue the business. Initiated by the Vienna Convention, this campaign was further enhanced by the creation of the Egmont Group and the FIU network when it was realized that the key to restrain dilatory prosecuting authorities was mutual international information sharing. Simultaneously, banking institutions experienced being fined for acting incautiously in relation to money laundering schemes. This was perceived as unjust since they were suspecting the ongoing crimes but had no options to report the offences due to professional secrecy rules. Action therefore needed to be taken to protect financial intermediaries from being associated with criminal activity. The initiative came with the launching of the Basle Committee Principles and shortly after by the creation of the FATF. Nothing illustrates that international AML
responds to a changing criminality picture better than the risk based approach adopted after September 11th 2001. The political environment after the terrorist attacks was left with the recognition that hitherto AML policies were not only insufficient, but the threat itself had changed. Focus therefore shifted from collecting evidence of financial crime to predict possible terrorist attacks through intensive electronic surveillance of financial activity.

The Wolfsberg Group initiative was also risk based, and stressed the benefits of identifying a common interest. In relation to the drafting of the Wolfsberg Principles, US and European banks had been convinced that a common AML standard was beneficial. At the early stages of international AML however, a rule based government approach based on a reactive, prescriptive strategy not universally suitable to all banking institutions was adopted. This led to uneven implementation of AML standards. Thus the Wolfsberg Group promoted a risk based approach designed and implemented in accordance with the specific needs and features of each banking institution (Pieth and Aiolfi 2003:6). Two leading banks made a first move by exchanging their policies which in turn formed a basis from which a common denominator was built. This kind of self-regulation resulted in convergence between regulators and the banking sector in developing AML strategies.

The indication of a common interest in collaborating against money laundering, whether in response to profit motives or a changing criminality picture, supports Keohane’s assumption that international regimes can persist in the absence of a hegemon. It was assumed that if this was the case, the three regime functions; mutual liability through recognized rules for behaviour, mutual information sharing and regime maintenance owing to cost reductions through comprehensive cooperation should be maintained by the FATF. Regarding regime maintenance, the AML nexus led by the FATF represents a solid apparatus for combating money laundering both in terms of policy frameworks and participation. This common denominator offer resource savings in terms of time, communication, information sharing and
decision making. Due to the costs of creating these standards, and since a common framework is more beneficial than negotiating several bilateral agreements, AML collaboration is likely to persist. Mutual liability is identified through the mutual evaluation procedures ensuring compliance with the 40 Recommendations. Mutual information sharing is encouraged by the 40 Recommendations (recommendations 35-40). This may be done through legal assistance, by coordinating seizure proceedings, and by implementing international conventions\textsuperscript{34}. The latter also serves as a carrot because share of confiscated assets is encouraged.

Mutual information sharing is also secured through the Egmont network of FIUs, and represents a factor which may encourage actors to overcome their reluctance to cooperate, consistent with interest based theories. By establishing the principle of mutual information sharing, an incentive for joining the AML campaign is created. International criminal networks conceal their proceeds in financial institutions that are not located in the country of crime commitment. This poses obstacles to investigation, thus the possibilities of receiving assistance in tracing the proceeds offered by mutual information sharing also serve as a carrot. Most countries facing the difficulties of detecting money laundering would be interested in providing information because they are interested in obtaining information due to the value of what can be received in return. However, traditions for information sharing are culturally embedded. For instance, as one of the leaders of a Moscow FIU is a former KGB agent, this person is bound to former national traditions of international cooperation and acts more reluctantly than others\textsuperscript{35}. This contributes to impede the progress of mutual information flows with Russia. Time and learning must be provided for such traditions to change, yet this period of transition can not be long-lasting in order to avoid accuses of non-compliance. In this context, those possessing the authority to sanction non-compliant actors contribute to avoid situations exemplary of the Prisoner’s Dilemma.

\textsuperscript{34} \url{http://www.fatf-gafi.org/pdf/40Recs-2003_en.pdf} \\
\textsuperscript{35} Information based on an interview with an AML official, June 2004.
Despite the recognition that AML collaboration is most beneficial, there are diverging opinions between countries on how to conduct collaboration. Because FATF power is represented not by one single country but by a group of countries having one equal vote each, the outcomes of cooperation can be object to bargaining between the most powerful actors. This is consistent with Keohane’s account and can be exemplified by the disagreements between Britain and Switzerland. Handing over responsibility to members countries through mutual evaluation procedures may contribute to evade the feeling of a top-down policy. More importantly, perceptions of participation as a common interest in order to evade problems related to the Prisoner’s Dilemma situation are created through this procedure. Because two countries subject to AML expect each other to choose competitive strategies and adopt a lower degree of compliance than required, they fail to pursue collaborative strategies and miss an optimal AML outcome. But mutual evaluation procedures prevent this dilemma.

4.4.3 The Positioning of Knowledge in International AML

“Cooperation can not be conducted unless there is consensus on the starting point”

-Else-Cathrine Lund, Økokrim

Entering into multilateral AML agreements can be a controversial issue because decisions need to be made across different national regulations concerning criminal law, professional secrecy and traditions for cooperation. This points to a social embedding of international AML and relates to knowledge based theories’ emphasis on how international relations arise as a reflection of the needs and interests of states and groups. Therefore, rationalist theories can be criticized for not taking into account that the countries, bodies and organizations involved in the project of collective prevention of money laundering consist of people with individual meanings. This can be illustrated by how AML professionals have influenced both application and design of technologies. For instance, rules of record keeping and suspicious

---

36 This was illustrated by the difficulties of getting information from a Moscow FIU and the disagreements between Switzerland and Britain in relation to the NCCT black-listing.
activity reporting rely on payment technologies as a source of information. Technology
design is exemplified by the electronic AML solutions implemented in Norway and the USA.
This indicates that AML technologies are both formed by people’s needs as well as they are
shaping people’s conduct, which is consistent with the accounts of Wyatt (1998) and

As indicated earlier in this thesis, the contribution of knowledge based theories to
international AML should be expected found in an emphasis on consensus knowledge
affecting AML policies. Consistent with Keohane, it has been demonstrated that this is not a
precondition for cooperation if there exists a hegemon in international AML, and it has been
illustrated that the FATF maintains the role of such a hegemon. However, this does not mean
that international AML lacks consensus knowledge. On the contrary, the information retrieved
from the empirical data collection reveals a strong emphasis on consensus knowledge, and
this knowledge is rooted in information commonly shared and provided by a group of experts.
It was also suggested that if international AML possesses the features of a technological
system, possibly the concept of technical authority would have more explanatory value in
describing the influence of expert knowledge on AML collaboration than epistemic
communities. The linkages between international AML and a technological system have
already been identified, thus technical authority should be more prevalent than epistemic
communities. However, the distinction between these two is not that straightforward. Both
concepts can be identified. Yet the one can be separated from the other in relation to AML
before and after September 11th 2001: scientific knowledge exemplary of epistemic
communities was prevalent before the terrorist attacks, while technical authority can be linked
to AML after the terrorist attacks. Three examples can be listed to indicate the relevance of
expert knowledge exemplary of epistemic communities in international AML. The FATF
decision-making process brings together the policy-making power of legal, financial and law
enforcement experts, and the papers on which decisions are based are prepared by professionals. Second, the intension of the annual FATF typologies on recent money laundering (and since 2001 counter-terrorist financing) techniques is to provide material to help FATF policy makers develop AML standards. The typologies exercises are based on topics that have been agreed on by the FATF Plenary, rooted in countries’ experiences, and culminate in an expert meeting. The findings from this expert meeting in turn serve as a basis for the information spread to regulatory, FIU and law enforcement agencies, as well as to the general public. Third, the SWIFT interbank reporting system is based on expert information collected from both public and private sectors including legal officials, financial institution authorities and software industry representatives in order to benefit from the knowledge held by the most specialised people in the world. The common denominator of these examples is that they are based on “transnational networks of specialists” exemplary of epistemic communities, and the experts referred to include scientists, law enforcement professionals, financial experts, diplomats as well as politicians.

As for the technical authority concept, this can be exemplified by how AML professionals defer to technology intensive models of risk assessment instead of relying exclusively on traditional sources of expert knowledge consistent with epistemic communities. This is particularly obvious in the risk based AML approach adopted after September 11th 2001. Expert knowledge is here safeguarded through scientific mathematical modelling on which “dataveillance” systems are built. FATF classifications can in this respect be said to have become computerized and integrated into these surveillance solutions, and as stated in de Goede (2004:12) “arguments, decisions, uncertainties and processual nature of decision-making are hidden away inside a piece of technology”. Whereas Haas’ idea of scientific knowledge influencing AML policies includes social conventions irrespective whether they

have emerged out of scientific, cultural or political factors, technical authority relates more specifically to scientific knowledge which does not emphasize political opinions. Rather, in relation to electronic AML solutions these political opinions are embedded in the technology, and the technical authority offered by these solutions contributes to increase policy makers’ confidence in a technical expert industry which in turn influences AML policies:

Software installs relatively unchangeable, taken-for-granted protocols in the day-to-day information practices of organizations, providing unified ways of interpreting events, influencing the ways in which decisions are made and standardizing such decisions over time and space (Leyshon & Thrift in de Goede 2004:13).

Yet this software can not be seen as independent of political ideas, since it was created in response to political needs. But by infiltrating such needs inside the software, perhaps technical authority can create perceptions of “objective” scientific knowledge. What secures the legitimacy of technical authority is its openness to peer review. Technical authority does not necessarily have to refer to technology. An example can be illustrated by directing attention to the FATF methodology for assessing compliance with the 40 Recommendations and the Eight Special Recommendations. It was developed in 2004 in collaboration with the IMF and the World Bank. Evidence of technical authority is that great effort was put in the design of a questionnaire attached to the methodology. Discussions were conducted in detail on the wording of the questionnaire to avoid that it was based on political opinions, in order to secure a common understanding of global standards for countries to adhere to. In this sense, technical authority can contribute to increase confidence in the integrity and rightness of the source of rules and in turn establish consensually shared knowledge. This indicates another difference between technical authority and epistemic communities. Whereas the latter alludes to a top-down strategy with regard to the inclusion of political intensions, the former indicates a bottom-up strategy due to its alleged linkages to a de-emphasis on political

---

38 Information based on an interview with an AML official, June 2004.
opinions and the openness to peer review which in this respect may create perceptions of scientific and not political knowledge. It has been demonstrated that expert knowledge exemplary of epistemic communities fits international AML before September 11th 2001, while technical authority is more relevant in explaining AML after the terrorist attacks. Yet the picture is not that unambiguous. This would mean that pre-September 11th AML was top-down in nature and post-September 11th AML was a bottom-up strategy. A quick flashback to the dataveillance systems currently being conducted in the USA weigh heavily against a bottom-up strategy though. However, an increased reliance on technological solutions in international AML suggests that technical authority has emerged as a way of creating consensus knowledge influencing AML policies. But it does not mean that epistemic communities are obsolete.

4.4.4 Path Dependence: the Predetermined Evolution of the Regime
It has already been argued that the AML regime is likely to persist partly due to the cost reductions of collaborating versus negotiating several bilateral agreements. But regime persistence must in this issue area also be seen in relation to its interrelatedness between human and technical factors, and its path dependence regarding its specific technical evolution. International AML is built on policies, exemplified by rules of record-keeping and suspicious activity reporting, but more importantly there must be people to design and use these rules. A prerequisite to rule application is that there are skilled people to conduct requests of information processing within and between financial institutions. This is in turn depending on networked electronic funds transfer technologies. The efficiency of these networked technologies depend on transaction costs, networked computers and their appurtenant software and hardware, optical fibres as well as innovations in microchip mass-production. Once these factors were established and carefully enmeshed in each other through coordination, international AML gained momentum as procedures for mutual behaviour were
put into practice. As such, the complexity and dynamics of international AML contributes to regime persistence. The crucial point is however that the evolution of the regime is bound to the problem underlying AML. As electronic payment technologies were first introduced, they were limited to banking institutions and were thus controllable. With the onset of financial liberalization and a subsequent universal application of financial sector payment technologies including internet banking and smart card usage however, the system has become more difficult to regulate and money launderers have been able to operate under circumstances in which their activities have been less likely to become unveiled. The momentum acquired by these technologies in turn serves as a necessary starting point of international AML. In order to attack money launderers where they are most vulnerable; at the placement stage, the dependence on these technologies (dataveillance solutions for instance) manifests itself. This is also evidence that international AML set out to solve a technical problem, which is one of Porter’s assumed ways in which regime formation can be influenced by technological systems. Moreover, it opposes rationalist theories’ emphasis on the choice among alternatives. In the context of international AML these choices are limited by the path dependence described above because AML professionals are “responding automatically to structural changes brought about by technological developments” (Porter 2003:531). The reasons for initiating enhanced action against money laundering were largely rooted in concerns with extensive use of the financial system for money laundering purposes. This indicates that the subsequent AML cooperation arose in response to such structural changes brought about by technological developments vulnerable to exploitation by criminals. International AML thus took on a form that was conditioned by the existing payment technologies.

4.4.5 Regime Effectiveness
It was indicated at the beginning of this chapter that for an international regime to have any relevance it must have some degree of effectiveness. International AML is only as successful
as the weakest link in the chain. The black-listing of NCCTs can be seen as a way of trying to secure AML efficiency. Williams & Baudin O’Hayon (2001:139) maintain that some of the participating countries and jurisdictions are in practice “part of the problem rather than part of the solution”. Relating to weak and criminal states, whether tied to domestic problems like unstable regimes, civil war, famine and the like, or corrupt states that simply rely on market survival by supporting criminal business\textsuperscript{39}, such countries hamper effective AML. Many countries within these categories also perceive international AML as a top-down policy from multilateral bodies acting on a level superior to their national governments. The irony of such a top-down policy is that less compliant countries often found in weak, corrupt or criminal states are easily stigmatized as the worst offenders whereas shortcomings within supposedly highly compliant member countries are toned down. For instance, a newspaper article from Norway shows that a sampling test to inspect compliance carried out in February 2004, reveals that out of twelve highly profiled financial institutions, only two could document satisfactory record keeping procedures, and only two had sufficient routines for personnel training\textsuperscript{40}. The admitted deficiencies of US domestic AML policies in relation to the launching of the naming and shaming list in 2000 also illustrates this.

According to Williams and Baudin-O’Hayon (2002:141) international AML is bound to inefficiency because of a FATF tendency to exalt form over substance by operating with procedural norms and standards before substantive norms with real impact. Achievements of international AML should however prove this perception wrong. On the contrary, the task force is perhaps the only international AML body that \textit{does} hold substance, which can be illustrated by the putting into practice of the Vienna Convention and the Basle Committee Statement of Principles. It is in any case too early to conclude that international AML is inefficient. Passing laws to implement international AML standards is not a time consuming

\textsuperscript{39} Nauru is one of the six FATF NCCTs and lives largely by protecting proceeds from the Russian mafia.

\textsuperscript{40} Dagens Næringsliv, 10.06.04 (http://avis.dn.no/). Retrieved on June 10th 2004.
issue as opposed to putting these into practise. The regulatory framework has only been around for a short period of time, thus the effects in terms of increased detection, confiscation and conviction can not be expected revealed before international regulations have been allowed to function in practice. Taking the social and cultural embedding of behavioural change into consideration this process will not take place over night. Without the contribution of the FATF there would be no AML regime. By bringing international conventions and directives into practice the FATF makes sure that the effort to curtail money laundering is more but a mere paper mill.
5 Conclusion

5.1 Summary
This thesis has demonstrated how electronic payment technologies can be used both to facilitate and fight money laundering. Major laundering techniques have been described, and important AML bodies and AML techniques have been accounted for. Apart from this, the research question behind this thesis was to decide if it exists an international AML regime which also possessed the features of a technological system, and how this affected AML. The thesis was introduced with a story from the real world revealing how corrupt banking sector executives assisted extensive money laundering schemes in relation to the Bank of New York scandal in the late 1990s. Unfortunately, it symbolizes the relevance of the topic and illustrates the presence of this crime in the financial sector. But more importantly, it illustrates why it is necessary to mobilise countermeasures. It has been demonstrated that collaborated international money laundering countermeasures can be labelled an international regime. An account was developed which maintains that international AML has linkages to a technological system, and that the features of this technological system influences AML policies. It turned out that the relevance of the different theoretical approaches must be seen in relation to different stages of international AML. Regime formation was explained by the hegemonic power of the USA at the early stages of international AML, but several incidents indicated that the USA also used its power to secure other countries’ compliance with international standards in later stages of the regime process, thus the USA contributes to regime maintenance. Despite criticism of a partly top-down policy from multilateral bodies controlled by the core of industrialized countries, it seems like an increasing number of countries are starting to recognize the benefit of collaborating against money laundering. The reasoning for this includes several factors: the fear of losing respectability which in turn severely affects business contributes to explain countries’ compliance with AML standards.
The benefits of receiving international assistance in catching crime perpetrators also serve as an incentive to adopt AML standards. This can be related to a desire of bringing back lost tax income kept in financial havens. But international AML must also be seen as a response to a changing criminality picture which requires corresponding countermeasures. It was argued that the AML regime can persist in absence of a hegemonic power, and important regime functions are maintained by the FATF. The role of knowledge in international AML was discussed, and in this context the concept of scientific knowledge exemplary of epistemic communities was opposed to the technical authority concept related to technological systems. A distinction can be made between the two regarding their relevance. It was determined that the former is suitable for explaining expert influence on AML policies before the terrorist attacks of September 11th 2001, whereas expert knowledge derived from technical authority best describes expert influence on international AML after this incident. It was stressed that this does not mean that epistemic communities are obsolete. The terrorist attacks symbolize a watershed in international AML. Whereas countermeasures previously focused on tracing criminal money after crime commitment, AML after September 11th 2001 is built on a risk based surveillance strategy seeking to predict possible terrorist attacks. Regime persistence can as mentioned partly be explained by US power. But an explanation was provided illustrating that the AML regime also is likely to persist due to its complexity and the cost reductions of operating out of a common starting point. Yet regime maintenance must be viewed in light of its path dependence in the sense that the natural AML starting point was conditioned by the technologies underlying money laundering, and that it therefore also is bound to follow its specific evolution. Although power politics are still in force, collaboration within this regime is largely technical in nature. Regarding regime effectiveness, it was argued that it is too early to draw the conclusion if international AML is efficient or not. The AML nexus entails an extensive regulatory framework which has been developed in the
course of less than two decades. Thus time must be provided to let these regulations function in practice before the results of collaboration in terms of seizure and confiscation can be expected.

5.2 Implications
Despite important achievements, the AML nexus has been object to criticism. What best illustrates this is the USA Patriot Act and its subsequent controversial infringement of civil rights in relation to financial surveillance strategies. It was argued that the concept of technical authority has the potential for establishing consensus knowledge by creating perceptions of a bottom-up strategy influencing AML policies. However, although US citizens would agree that the threat posed by terrorism legitimizes more far-reaching countermeasures, as illustrated by the dataveillance systems this consensus is not publicly shared. The difference between AML requirements before and after the terrorist attacks in New York and Washington is that policy makers now are willing to adopt drastic measures even if this entails violation of the civil rights of its people. AML/anti-terrorist standards subject to the Patriot Act are therefore involuntarily adopted.

The FATF naming and shaming strategy was abandoned in 2003 and replaced by a more inclusive audit conducted by the IMF, built on voluntariness. The fact that more than 100 countries shortly after addressed the IMF requesting assistance in establishing AML policies may indicate that countries increasingly are acknowledging the benefits of adhering to international standards. But more importantly, although the black-listing of NCCTs undoubtedly was efficient, the IMF audit might contribute to reduce perceptions of a top-down policy.

These two implications call for the importance of finding a legitimate balance between what it takes to combat money laundering and terrorist financing effectively and how far one is willing to go in reaching that goal. The IMF experience suggests that a strategy based on
voluntariness where participants actively seek advice on how to reach compliance with international standards is a more legitimate way of conducting collaboration as opposed to sanctioning methods. This bottom-up strategy supports the assumption that regime maintenance is rooted in a common interest, although the USA highly conducts the AML campaign. It can however be asked if a certain degree of coercion perhaps is necessary in order to create deterrence and general prevention effects, exemplified by increased concerns with financial reputation and international acceptance. In any case, this is an issue area which requires research on the actual follow-up of AML standards. The sampling test of twelve Norwegian financial institutions revealed that a country which is otherwise devoted to international requirements failed to fulfil its obligations. Not only does this require research on follow-up, but also follow-up of financial institutions in itself. This in turn is a resource demanding task in terms of people, time and money, but initiating an extensive offensive against money laundering and terrorist financing can not be successful if regulative frameworks are not followed up at the other end.
## Appendix A: List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-money Laundering</td>
</tr>
<tr>
<td>BIS</td>
<td>Bank for International Settlements</td>
</tr>
<tr>
<td>ESST</td>
<td>European Inter-University Association on Society, Science and Technology</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force against Money Laundering</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>FSF</td>
<td>Financial Stability Forum</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>GPML</td>
<td>Global Programme against Money Laundering</td>
</tr>
<tr>
<td>G7</td>
<td>Group of Seven</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communication technologies</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>NCCT</td>
<td>Non-cooperative Countries and Territories</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>OFC</td>
<td>Offshore Financial Centres</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>SCOT</td>
<td>Social Construction of Technology</td>
</tr>
<tr>
<td>STS</td>
<td>Science, Technology and Society</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunications System</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office for Drug Control and Crime Prevention</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
Appendix B: List of Interviewees

- Representative from the SAS Institute AS: Director of Strategy and Business Development Dr.Sc. Inge Krogstad
  Interviewed on June 1st 2004.

- Former Representative from the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime:
  Senior Consultant Geir Olderbakk
  Interviewed on June 2nd 2004.

- Representative from the Financial Supervisory Authority of Norway:
  Special Adviser Rune Grundekjøn
  Interviewed on June 8 2004.

- Representative from Accenture, Finance and Performance Management:
  Associate Partner Anne Steen
  Interviewed on June 11 2004.

- Representative from the Norwegian Financial Services Association:
  Deputy Director Hans-Jacob Anonsen
  Interviewed on June 17 2004.

- Representative from the Ministry of Justice and the Police and the Norwegian FATF delegate: Deputy Assistant Secretary General Anne-Mette Dyrnes

- Representative from the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime:
  Police Prosecutor Else-Cathrine Lund
  Interviewed on June 28 2004.
Appendix C: Definition of Financial Institutions

“Financial institutions” means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.
3. Financial leasing.
4. The transfer of money or value.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   a. money market instruments (cheques, bills, CDs, derivatives etc.);
   b. foreign exchange;
   c. exchange, interest rate and index instruments;
   d. transferable securities;
   e. commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.

Source: http://www.fatf-gafi.org/40Recs_en.htm#Financial%20institutions
References


Electronic sources

http://avis.dn.no/

http://www.bis.org

http://www.bis.org/publ/bcbsc102.pdf

http://www.fatf-gafi.org

http://www.fatf-gafi.org/AboutFATF_en.htm#Decision-Making

http://www.fatf-gafi.org/NCCT_en.htm

http://www.fatf-gafi.org/40Recs_en.htm


http://www.fatf-gafi.org/MLaundering_en.htm


http://www.fsforum.org/home/home.html

http://education.yahoo.com/reference/dictionary/entries/33/d0273300.html

http://www.egmontgroup.org/


http://encarta.msn.com/dictionary_1861733097/shell_company.html

http://europa.eu.int/comm/internal_market/en/finances/banks/01-1580.htm

http://www.heritage.org/Research/TradeandForeignAid/EM623.cfm


http://www.imolin.org/imolin/gpml.html

http://www.interpol.int/Public/Icpo/default.asp

http://www.oecd.org

http://www.russianlaw.org/crisis.htm

http://www.swift.com/index.cfm?item_id=41756

http://www.unodc.org/unodc/money_laundering.html


http://www.wolfsberg-principles.com/