1. Introduction

Money laundering (ML) has long been recognized as an important contemporary phenomenon and a challenging problem area. Institutions have been organizing their responses to targeting ML for some time, however these efforts have intensified over the past two decades. Following the arbitrary connection made between the financing of terrorism and money laundering, a renewed interest in the topic has emerged within the broader agenda of dealing with security issues.

Despite the continuous efforts against ML, encouraging results have not really been witnessed; prosecutions are scarce and convictions even scarcer. Although the network of stakeholders involved in anti-money laundering (AML) has expanded due to a wide range of regulatory initiatives, such an expansion has come with a number of practical difficulties for these stakeholders (that is professions like lawyers, accountants and so on) and the regulators that are supposed to check compliance against AML legislation. For most practical purposes, it would be difficult not to accept that financial institutions remain at the forefront of the fight. Consequently, the study of how financial institutions deal with this important problem domain remains crucial. However, financial institutions do not exist in a void. They are part of a complex socio-political and economic environment that, although advancing in particularly structured ways, faces unstructured consequences.

A considerable part of this lack of structure is due to the widespread penetration of technology into traditional organizations. Technology has transformed the way we operate within an organization, but more importantly, it has created a new platform for orchestrating information utilization and its management. Of course, technology as broadly understood has little to do with both the wider study of information systems, and the very concept of systems as developed and analysed in this book. Still, our dependence on technology has increased considerably, and it is evident that a technology that fails to function no longer comes to a complete halt; technology does however trigger unanticipated effects of a possibly catastrophic scale. Such effects not only undermine the operations of those stakeholders adopting technology; they also influence other stakeholders and their respective functional operations. We will come to
Technology and anti-money laundering

see how these effects permeate problem domains like AML, but also, and even worse, how they go unnoticed or become masked as an operational success. Hence, in a large number of fields (AML is no exception), society has come to rely on the functioning of technology, and has developed its own structures more and more on the basis of this precondition of reliance. This technological precondition is not just limited to AML. Financial institutions have always been technologically astute and have adapted their own organizational structures to include technological developments.

The current conditions in the broader AML domain appear to have acquired a highly unstructured complexity. This complexity is partly due to the regulatory initiatives that have spawned a myriad of reactions, and partly to the various technologies that have assisted in automating organizational processes. Such complexity is also amplified by an unrestrained opportunism shown by the software industry, which for a number of years has exploited the fact that technology was deemed by regulators as a necessary tool in the development of the fight against ML. Considerable but unplanned automation of operations for identifying suspicious transactions has resulted in a series of adverse effects for Financial Intelligence Units (FIUs), the stakeholders responsible for receiving the suspicious reports. Last but not least, the introduction of the risk-based approach with the 3rd AML Directive by the European Union (EU) has created a multitude of additional ambiguities. Even though the EU has rightly taken the step of introducing a more flexible approach, a series of difficulties and uncertainties have been introduced in how such a risk-based approach should be implemented. Financial and other institutions, as well as FIUs are having a rather difficult time making sense of this newly-born complexity that comes with the very elusive nature of risk. To put it simply, no one knows how to go about introducing, supervising and managing a risk-based approach for AML as the underlying infrastructure for doing so is simply non-existent. This is heavily supported by the popular delusion that we understand what risk is and how it can be managed. Such a strong assertion is not carried out here with the purpose of overemphasizing the problems. This section merely remains a brief introduction to the arguments that will be put forward as this book develops. The reality however also remains that feedback between FIUs and financial institutions is at a primordial state, interoperability issues are barely considered and stakeholder fragmentation as well as the sharing of intelligence is left unattended.

Within this dynamic between regulatory initiatives and technological adoption, the domain of AML is facing constant reconstruction. Much like a biological organism that encodes its own survival and evolution
within a double helix of a genetic code, the anti-money laundering system becomes structurally coupled with the system of technology with which it co-evolves. This interplay implies that the systems theoretical nature of AML and technology needs to be established and examined. Beyond the realm of technology, as it is commonly perceived, this book seeks to offer an insight into the broader effects that various information systems have within a financial institution in relation to AML. This implies that the commonly perceived technological platforms that currently affect ML, those of profiling technologies that attempt to simulate money laundering behaviour, remain but a single instance of a much larger infrastructure of various computerized information systems that have similar (if not more powerful and propagating) effects on AML.

This book sets out to examine the following issues regarding AML:

1. What theoretical description can be developed in order to describe the domain of anti-money laundering through the lens of systems theory?
2. What is the role that various information systems come to occupy within financial institutions? How do the complex interactions between various information systems employed affect AML?
3. What is the nature of the risk-based approach, and what are the problems behind any attempt to model the concept of risk?

In seeking to outline the path for answering these questions, a general literature review is provided that deconstructs the problem of money laundering, while reviewing the issue of defining ML itself, estimating the ML market, reviewing some key legislative initiatives, and outlining global AML characteristics. This general review is done in Chapter 2.

Chapter 3 presents the key theoretical principles of systems theory. These constitute the foundational basis for developing the theory further and for relating systems principles to AML.

Chapter 4 describes the empirical findings of a longitudinal case study carried out in a major financial institution in the EU-area. The various computerized information systems influences are discussed in order to ponder the second research question outlined above.

Chapter 5 analyses a number of systems theory instances that lead to a description of AML as a system. There is an attempt to synthesize, in systemic terms, both the domain of AML and the domain of technology, all the while examining their interplay.

The book concludes with Chapter 6 where a treatise on the risk-based approach is presented, followed by a data-mining application and a number of conclusive arguments.